世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G11B 7/00, 20/10, 7/26, 20/12	A1	(11) 国際公開番号	WO96/16401
		(43) 国際公開日	1996年5月30日(30.05.96)

(21) 国際出願番号 PCT/JP95/02339
(22) 国際出願日 1995年11月16日(16.11.95)

(30) 優先権データ

特願平6/283415	1994年11月17日(17.11.94)	JP
特願平7/16153	1995年2月2日(02.02.95)	JP
特願平7/261247	1995年10月9日(09.10.95)	JP

(71) 出願人
松下電器産業株式会社
(MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)[JP/JP]
〒571 大阪府門真市大字門真1006番地 Osaka, (JP)
(72) 発明者
大嶋光昭(OSHIMA, Mitsuaki)
〒615 京都府京都市西京区桂南巽町115-3 Kyoto, (JP)
後藤芳秒(GOTOH, Yoshiho)
〒536 大阪府大阪市城東区東中浜4丁目9番17号201号室
Osaka, (JP)
(74) 代理人
弁理士 松田正道(MATSUDA, Masamichi)
〒532 大阪府大阪市淀川区宮原5丁目1番3号
新大阪生島ビル Osaka, (JP)

(81) 指定国
CN, JP, KR, MX, 欧州特許(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

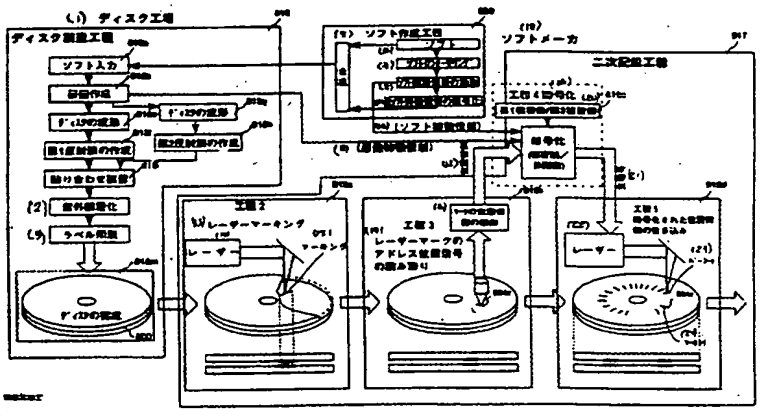
添付公開書類 国際調査報告書

(54) Title : MARKING GENERATING APPARATUS, METHOD OF FORMING LASER MARKING ON OPTICAL DISK, REPRODUCING APPARATUS, OPTICAL DISK AND OPTICAL DISK PRODUCING METHOD

(54) 発明の名称 マーキング生成装置、光ディスクのレーザーマーキング形成方法、再生装置、光ディスク、及び光ディスク製造方法

(57) Abstract

The invention improves the duplication prevention capacity in comparison with the prior art. In the optical disk according to the present invention, for example, marking is made on a reflection film of the disk on which data are written by a laser beam, at least the position information of the marking or information on the position information is written on the disk in the form of cipher or digital signature.



(1) ... disk factory
(2) ... cure disk with UV
(3) ... print label
(5) ... synthesis
(6) ... software
(7) ... author software
(8) ... extract software characteristic information
(9) ... cipher software characteristic information
(10) ... software characteristic information
(11) ... original disk characteristic information
(12) ... position information
(13) ... laser marking
(14) ... laser
(15) ... marking
(16) ... detect position information of mark
(17) ... read address position signal of laser mark
(18) ... software maker
(19) ... step 4 ciphering
(20) ... ciphering (secret key/open key)
(21) ... main cipher
(22) ... laser
(23) ... bar code
(24) ... marking
800 ... completion of disk
815 ... disk production process
817 ... secondary recording step
818a ... input software
818b ... produce original disk
818c ... mold disk
818f ... produce first reflective film
818i ... bonding
818g ... mold disk
818h ... produce second reflective film
819a ... step 2
819b ... step 3
819c ... first secret key/second secret key
819d ... step 5, write ciphered position information
820 ... software production step

（５７）要約

複製防止能力を従来に比べてより一層向上させることが出来る、マーキング生成装置、光ディスクのレーザーマーキング形成方法、再生装置、光ディスク、及び光ディスク製造方法を提供すること。そのために、例えば本発明の光ディスクは、データの書き込まれたディスクの反射膜にレーザーによりマーキングが施されており、少なくともそのマーキングの位置情報又はその位置情報に関する情報が、暗号化され、あるいはディジタル署名された形で、前記ディスクに書き込まれている。

情報としての用途のみ

ＰＣＴに基づいて公開される国際出願をパンフレット第一頁にＰＣＴ加盟国を同定するために使用されるコード

AL	アルバニア	DK	デンマーク	LK	スリランカ	PT	ポルトガル
AM	アルメニア	DE	ドイツ	LR	リベリア	RO	ルーマニア
AT	オーストリア	EE	エストニア	LS	レソト	RU	ロシア連邦
AU	オーストラリア	ES	スペイン	LT	リトアニア	SD	スーダン
AZ	アゼルバイジャン	FI	フィンランド	LU	ルクセンブルグ	SE	スウェーデン
BA	ボスニア・ヘルツェゴビナ	FR	フランス	LV	ラトヴィア	SG	シンガポール
BB	バルバドス	GA	ガボン	MC	モナコ	SI	スロヴェニア
BE	ベルギー	GB	英国	MD	モルドバ	SK	スロヴァキア共和国
BF	ブルキナ・ファソ	GE	グルジア	MG	マダガスカル	SL	シエラレオネ
BG	ブルガリア	GN	ギニア	ML	マリ	SN	セネガル
BJ	ベナン	GR	ギリシャ	MN	モンゴル	SZ	スワジランド
BR	ブラジル	HU	ハンガリー	MR	モーリタニア	TD	チャード
BY	ベラルーシ	IE	アイルランド	MW	マラウイ	TG	トーゴ
CA	カナダ	IS	アイスランド	MX	メキシコ	TJ	タジキスタン
CF	中央アフリカ共和国	IT	イタリア	NE	ニジェール	TM	トルクメニスタン
CG	コンゴー	JP	日本	NL	オランダ	TT	トリニダード・トバゴ
CH	スイス	KE	ケニア	NO	ノルウェー	TZ	タンザニア
CI	コート・ジボアール	KG	キルギスタン	NZ	ニュージーランド	UA	ウクライナ
CM	カメルーン	KP	朝鮮民主主義人民共和国	PL	ポーランド	UG	ウガンダ
CN	中国	KR	大韓民国			US	米国
CZ	チェッコ共和国	KZ	カザフスタン			UZ	ウズベキスタン共和国
DE	ドイツ	LI	リヒテンシュタイン			VN	ヴィエトナム

明 細 書

マーキング生成装置、光ディスクのレーザーマーキング形成方法、再生装置、光ディスク、及び光ディスク製造方法

技術分野

本発明は、たとえば、光ディスクの複製防止に利用可能な、マーキング生成装置、光ディスクのレーザーマーキング形成方法、再生装置、光ディスク、及び光ディスク製造方法に関するものである。

背景技術

近年、ＲＯＭ型光ディスクの普及に伴い、海賊版ディスクが登場し、著作権者の権利を侵害している。

これは、ＲＯＭディスクの製造装置が容易に入手できるようになり、かつ操作が簡単になったことによる。

海賊版業者は、ＣＤのソフトの論理データのみを抽出し、磁気テープに落とし、原盤作成装置にセットするだけで、ＣＤの原盤ができる。この１枚の原盤をもとに数十万枚の海賊版ディスクがプレス成形できる。この場合、海賊版業者は著作権料を支払わないため安い価格で海賊版ディスクを販売し、利益を上げている。当然、この分だけ著作権者は損害を被ることになる。

今のＣＤ規格においては、ＣＤの論理データを読み出す機能しかなく、ディスクの物理的特徴を検出する機能をもってない。このため論理データをビット複写によりコピーするだけで、海賊版ＣＤが作成できる。

この物理的特徴を識別する機能を追加することにより、海賊版を防止する方法

が従来技術として知られている。

これは、原盤に物理的なマークを加える規格を新たに作ることにより、この規格のディスクの海賊版の製造を防止する。従来例として特開平５－３２５１９３に示すような海賊版防止方式が知られている。この方式はカッティング時に、意図的に特定の領域の記録時に記録ビームをトラッキング方向に走査させ、ウォブリングを原盤上に形成する。このディスクを再生する時は再生プレーヤ側で、ウォブリング検出回路を設け、このウォブリングが特定の領域にあるかどうかをチェックする。特定のウォブリング周波数のウォブリングが特定の領域にある場合は正規ディスク、ない場合は海賊版ディスクと判断する。

つまり、ウォブリング機能をもつ特殊な原盤製造装置を用いて、予め設定された物理マークの設計データに基づき、原盤にその物理マークを作成するものである。従って、海賊版業者はこの特殊な原盤製造装置も物理マークの設計データも、もってないため、海賊版ディスクを製造できない。この場合、この規格のディスクには全て海賊版防止マークをつける必要がある。しかし、この物理マークは正規ディスクを観察することにより得られるので、この特殊な原盤製造装置を海賊版業者が入手した段階で海賊版が製造されるという問題点があった。本明細書ではこの原盤に物理マークを設けるタイプの海賊盤防止方式を原盤レベル方式と呼ぶ。

他にも、この原盤レベル方式でさらに複雑な物理マークを作成する方法が提案されている。しかし、原盤レベルで如何に複雑な物理マークを作成しても、正規ディスクの樹脂を溶かして、直接全く同じ物理形状のレプリカを作成する原盤複製方法であるレプリカ方式が知られている。この方法は原盤１枚を複製するのに時間がかかり、高コストであるが、海賊版原盤１枚から数十万枚のディスクが成

形できるので、海賊版ディスク１枚あたりのコストは安い。従って、今後登場するレプリカ方式の普及に伴い、原盤レベルの海賊版防止技術の防止効果が無意味化するという問題点があった。

以上のように、従来の海賊版防止技術にはいくつかの課題があることがわかる。

以下、これらの課題をまとめる。

課題１として、従来の、原盤レベルの海賊盤防止方式の物理マークはレプリカ複製が可能なため、防止効果が低い。

課題２として、物理マークの設計データに基づき、物理マークを作成する従来方法では正規ディスクメーカと同じ精度の製造装置を入手することにより、容易に海賊版を製造できる。

課題３として、従来の海賊盤防止方式は安全性のレベルが固定されているため、時代の経過とともに向上する海賊版技術に対して効果が低下する。

課題４として、防止機能のついているディスクフォーマットとついていないディスクフォーマットの双方を認めると防止機能のついていないディスクフォーマットで海賊版ディスクが製造される。このため、全てのディスクに防止機能をつける必要があった。ゲーム規格ディスクのように閉じた規格に限定されている。

課題５として、従来方式では一部のライセンス親会社が特殊な製造装置をもち、公開しない。このため、各ソフトメーカは親会社でしかディスクを製造できない。

課題６として、原盤マーク方式では１枚の原盤に対して成形されたディスクは全て同じディスクＩＤをもつ。つまり、１つのパスワードで他のディスクが動作する。このため、フロッピィや通信回線を併用しないとパスワードセキュリティが保てない。また、二次記録できないため、パスワードを毎回入力する必要があった。

発明の開示

本発明は、上記従来の課題を考慮し、複製防止能力を従来に比べてより一層向上させることを目的とする。

即ち、本発明では、上記の従来の海賊版防止方式の６つの課題を解決するために、以下の手段を提供する。

まず、課題１に対しては、従来の原盤レベルの物理マークに代わるものとして、ディスクの反射膜に物理マークを設ける反射膜レベルの物理マークによる海賊版防止方式を提供する。これにより、原盤レベルで複製されても海賊版が防止できる。

課題２に対しては、２枚貼り合わせＲＯＭディスクにレーザーで二次記録する新しいＲＯＭ記録手段を用いる。まず、第１ステップでランダムに物理マークを作成し、次に第２ステップで０．１３μｍの高い測定精度で、物理マークを測定する。第３ステップでこの位置情報を暗号化して上記二次記録手段を用いてＲＯＭディスクに数十μｍ、つまり通常の加工精度でバーコード記録する。こうして通常の装置の加工精度をよりはるかに高い精度、例えば０．１μｍの光マーク位置情報が得られる。市販の加工光マークをこの０．１μｍの精度で加工することはできないため海賊版の製造は防止される。

課題３に対しては位置情報をデジタル署名暗号化した暗号として、ディスク上に安全度の低い第１世代の暗号と安全度の高い第２世代の暗号の双方を、予め記録する媒体を用いることにより、世代の異なる再生装置においてもその世代に対応した暗号の安全度で海賊版を防止する。

課題４に対してはそのソフトに対して著作権が海賊版防止機能を付与したか、

してないかを示す海賊版防止機能識別子を原盤に記録する。この識別子が改ざんされないように、原盤にソフトコンデンツを記録する際にソフトコンテンツの圧縮情報とこの海賊版防止識別子をスクランブルして暗号化して記録する。この識別子が改ざんできないため海賊版非対策ディスクフォーマットのディスクを海賊版業者が作成できない。従って海賊版の製造が防止される。

課題５に対しては、ディスク製造に不可欠なデジタル署名暗号の秘密鍵に関してマスタ鍵よりサブ鍵を生成し、各ソフトメーカにサブ鍵を渡すことにより、サブ鍵によりソフトメーカが自社の工場で正規ディスクを製造できる。

課題６に対しては、本発明のディスク毎に異なる海賊版防止マークの位置情報をディスク識別子として用いる。位置情報とディスクのシリアル番号、つまりディスクＩＤを合成して、デジタル署名暗号化することにより改ざんできないディスクＩＤを一枚毎に付与する。完成ディスク１枚毎にＩＤが異なるため、パスワードも異なる。従って、他のディスクでは、このパスワードは動作しないため、パスワードセキュリティが向上する。

また、本発明の二次記録により、パスワードをディスクに二次記録することによりそのディスクは永久に動作可能となる。

以上６つの課題を解決する具体的な方法を実施例を用いて以下に開示する。

本発明は、ディスクに形成された反射膜にマーキングを施すマーキング生成手段と、前記マーキングの位置を検出するマーキング位置検出手段と、前記検出された位置をマーキングの位置情報として出力する位置情報出力手段とを備えたマーキング生成装置である。

又、本発明は、少なくとも前記出力された位置情報又はその位置情報に関する情報を前記ディスクに、又は別の媒体に書き込むための位置情報書き込み手段を

備えたマーキング生成装置である。

又、本発明は、ディスクの成形を行うステップと、前記成形されたディスクに反射膜を形成するステップと、前記反射膜が形成されたディスクを少なくとも1つ含む2枚のディスクを張り合わせるステップと、その張り合わされたディスクの前記反射層に対して、レーザーによりマーキングの形成を行なうステップとを備えた光ディスクのレーザーマーキング形成方法である。

又、本発明は、ディスクに形成された反射膜にマーキングを施し、前記マーキングの位置を検出し、少なくとも前記検出された位置がマーキングの位置情報として出力された、そのマーキングの位置情報又はその位置情報に関する情報を読み取る位置情報読み取り手段と、前記マーキングの現実の位置に関する情報を読み取るマーキング読み取り手段と、前記位置情報読み取り手段による読み取り結果と、前記マーキング読み取り手段による読み取り結果とを利用して、それらを比較判定する比較判定手段と、前記比較判定手段の比較判定結果に基づいて、前記光ディスクの記録データを再生する再生手段とを備えた再生装置である。

又、本発明は、ディスクの成形を行うステップと、前記成形されたディスクに反射膜を形成するステップと、前記反射膜に対してマーキングを施すステップと、前記マーキングの位置を検出するステップと、前記検出された位置をマーキングの位置情報として出力し、暗号化して前記ディスクに書き込むステップとを備えた光ディスク製造方法である。

又、本発明は、ディスクの成形を行うステップと、前記成形されたディスクに反射膜を形成するステップと、前記反射膜に対してマーキングを施すステップと、前記マーキングの位置を検出するステップと、前記検出された位置をマーキングの位置情報として出力し、その位置情報に関連してディジタル署名して前記ディ

スクに書き込むステップとを備えた光ディスク製造方法である。

又、本発明は、データの書き込まれたディスクの反射膜にレーザーによりマーキングが施されており、少なくともそのマーキングの位置情報又はその位置情報に関する情報が、暗号化され、あるいはディジタル署名された形で、前記ディスクに書き込まれている光ディスクである。

又、本発明は、レーザにより消滅しない材料からなる２つの部材により反射膜が直接又は間接的に挟まれた構造を備えたディスクであって、その反射膜にレーザーによりマーキングが施されている光ディスクである。

図面の簡単な説明

第１図は本実施例におけるディスクの製造工程と二次記録工程図である。

第２図（ａ）は実施例におけるディスクの上面図、（ｂ）は実施例におけるディスクの上面図、（ｃ）実施例におけるディスクの上面図、（ｄ）実施例におけるディスクの横断面図、（ｅ）実施例における再生信号の波形図である。

第３図は本実施例における、暗号化された位置情報をディスク上にバーコードにより記録する工程のフローチャート図である。

第４図は本実施例におけるディスクの作成工程及び二次記録工程図（その１）である。

第５図は本実施例におけるディスクの作成工程及び二次記録工程図（その２）である。

第６図は本実施例における２層ディスクの作成工程図（その１）である。

第７図は本実施例における２層ディスクの作成工程図（その２）である。

第８図（ａ）は本実施例における張り合わせタイプの無反射部の拡大図、（ｂ）

は本実施例における単板タイプの無反射部の拡大図である。

第９図（ａ）は本実施例における無反射部の再生波形図、（ｂ）は本実施例における無反射部の再生波形図、（ｃ）は本実施例における無反射部の再生波形図である。

第１０図（ａ）は本実施例における張り合わせタイプの無反射部の断面図、（ｂ）は本実施例における単板タイプの無反射部の断面図である。

第１１図は本実施例における無反射部の断面を、透過電子顕微鏡により観察した結果を基にした模式図である。

第１２図（ａ）は本実施例におけるディスクの断面図、（ｂ）は本実施例におけるディスクの無反射部の断面図である。

第１３図（ａ）は同実施例における正規のＣＤのアドレスの物理配置図、（ｂ）は同実施例における不正に複製されたＣＤのアドレスの物理配置図である。

第１４図は実施例におけるディスク作成とディスク作成のブロック図である。

第１５図は実施例における低反射部位置検出部のブロック図である。

第１６図は実施例における低反射部のアドレス・クロック位置検出の原理図である。

第１７図は実施例における正規ディスクと複製ディスクの低反射部アドレス表の比較図である。

第１８図は実施例における一方向関数によるディスク照合のフローチャート図である。

第１９図は実施例における原盤別アドレスの座標位置の比較図である。

第２０図は実施例における低反射位置検出プログラムのフローチャート図である。

第２１図は同実施例の磁気記録装置のブロック図である。

第２２図は同実施例におけるＲＳＡ関数を用いた場合の暗号化等についてのフローチャート図である。

第２３図は同実施例における楕円関数を用いた場合のディジタル署名等についてのフローチャート図である。

第２４図は同実施例における位置情報の照合プロセスのフローチャート図である。

第２５図は同実施例における情報処理装置のブロック図である。

第２６図は同実施例における第２低反射部の上面図である。

第２７図は本実施例における１層目のマーキング信号の検出波形図である。

第２８図は本実施例における２層目のマーキング信号の検出波形図である。

第２９図は本実施例におけるディスク作成装置のブロック図である。

第３０図は本実施例における無反射部の符号図である。

第３１図は本実施例における無反射部の検出波形図である。

第３２図は本実施例におけるバーコード記録情報の内容及び相互関係の説明図である。

第３３図は本実施例における二層ディスクの無反射部の斜視図である。

第３４図は本実施例における流通におけるデータの流れを説明する図である。

第３５図は本実施例における流通におけるディスクの流通図である。

第３６図は本実施例における位置情報などをマスタ鍵とサブ鍵等を用いて、複雑に暗号化する場合の、製造過程を説明するブロック図である。

第３７図は本実施例における位置情報などをマスタ鍵とサブ鍵等を用いて、複雑に暗号化する場合の、製造過程を説明するブロック図である。

第３８図は本実施例における再生装置におけるフローチャート図である。

第３９図は本実施例における光ディスクに秘密鍵系と公開鍵系を併用した場合の、再生装置との関係を示す図である。

第４０図は本実施例における、光ディスクについて、位置情報などをマスタ鍵とサブ鍵等を用いて暗号化したものを記録し、再生する場合のアウトラインを示すブロック図である。

第４１図は本実施例における光ディスクの再生装置のブロック図である。

第４２図は本実施例のプログラムインストールにおけるスクランブル識別子の動作とドライブＩＤとディスクＩＤの切り換えを示すフローチャート図である。

発明を実施するための最良の形態

以下、本発明にかかるマーキング生成装置、光ディスクのレーザーマーキング形成方法、再生装置、光ディスク、及び光ディスク製造方法の実施例を構成と動作を伴せて説明する。

本実施例では、先ず、前半部（１）において、ディスクを作成すること、レーザを利用してマーキングを作成すること、そのマーキングの位置情報を読み取ること、さらにその位置情報等を暗号化等して光ディスクに書き込むこと、そしてその光ディスクのプレーヤ側の再生動作などについて述べる。なお、その暗号化の点と再生動作に関しては簡単に述べる。

次に、後半部（２）において、その簡単に述べられた、マーキング位置情報等の暗号化等、光ディスクの位置情報等復号再生等について詳細に説明する。又、その他の、海賊版防止に関する様々な工夫についても述べる。

なお、本明細書においては、レーザートリミングはレーザーマーキングとも呼

び、光学マーキング無反射部は単に、マーキング、あるいは光学マーキング、ディスク固有の物理ＩＤ等とも呼ぶ。

（1） 第１図は、ディスク作成工程から光ディスクの完成までの全体の大きな流れを示すフローチャートである。

まずソフト会社がソフト制作８２０においてソフトのオーサリングを行う。完成したソフトは、ソフト会社から、ディスク製造工場に渡される。そして、ディスク製造工場のディスク製造工程８１６では、ステップ８１８ａで完成したソフトを入力して、原盤を作成し（ステップ８１８ｂ）、ディスクを成形し（ステップ８１８ｅ、ステップ８１８ｇ）、それぞれのディスクに反射膜を作成し（ステップ８１８ｆ、ステップ８１８ｈ）、それら２枚のディスクを貼り合わせて（ステップ８１８ｉ）、ＤＶＤやＣＤ等のＲＯＭディスクを完成させる（ステップ８１８ｍ等）。

このようにして完成したディスク８００は、ソフトメーカーもしくはソフトメーカーの管理下にある工場に渡され、二次記録工程８１７においては、第２図に示すような、海賊版防止のマーキング５８４を施された後（ステップ８１９ａ）、測定手段によりこのマークの正確な位置情報を読み取り（ステップ８１９ｂ）、ディスク物理特徴情報としての位置情報を得る。ステップ８１９ｃでこのディスク物理特徴情報を暗号化する。ステップ８１９ｄでは、この暗号をＰＷＭ変調した信号をレーザにより、バーコード信号としてディスク上に記録する。なおステップ８１９ｃでソフトの特徴情報とディスク物理特徴情報を合成した情報を暗号化してもよい。

さらに、上記各工程を詳しく具体的に述べる。すなわち、第４図、第５図、第８図～第１２図などを用いて本発明による詳細な光ディスクのディスク作成工程

とマーキング作成工程とマーキング位置読み取り工程と暗号書き込み工程を説明する。尚、第６図、第７図を用いて、反射層が２つある場合について、補足説明を加える。また、ここでマーキング作成工程とマーキング位置読み取り工程と書き込み工程を総合して二次記録工程と呼ぶ。

（A）まず、ディスク作成工程について説明する。第４図に示すディスク作成工程８０６では、工程（１）で、透明基板８０１を成形する。工程（２）でアルミや金等の金属をスパッタリングさせ、反射層８０２を形成する。別の工程で作成した基板８０３に紫外線硬化樹脂の接着層８０４をスピンコートにより塗布し、反射層８０２をもつ透明基板８０１と張り合わせた後、高速回転させ張り合わせ間隔を均一にさせる。外部から紫外線を照射することにより硬化し、２枚は固く接着される。工程（４）でＣＤやＤＶＤのタイトルが印字された印刷層８０５をスクリーン印刷やオフセット印刷で印刷する。こうして、工程（４）で通常の貼り合わ型の光ＲＯＭディスクが完成する。

（B）次に、第４図と第５図を用いて、マーキング作成工程について説明する。第４図において、ＹＡＧ等のパルスレーザー８１３を用いて、集束レンズ８１４によりレーザー光を反射層８０２近傍に集束させることにより、第５図の工程（６）に示すように無反射部８１５を形成する。即ち、第５図の工程（６）において形成された無反射部８１５から工程（７）の波形（A）に示すように顕著な波形が再生される。この波形をスライスすることにより波形（B）のようなマーキング検出信号が得られ、信号（d）に示すようなアドレス、そして、信号（e）に示すようなアドレス、フレーム同期信号番号、再生クロック数の階層的なマークの位置情報が測定できる。

尚、ここで、上述したように、第６図、第７図を用いて、別のタイプのディス

ク（２層式の張り合わせディスク）について、補足説明を加える。

即ち、第４図、第５図は、反射層が片側の基板８０１にのみ形成されるいわゆる一層式の張り合わせディスクの場合を示していた。これに対して、第６図、第７図は、反射層が、基板８０１、８０３の両方に形成される、いわゆる２層式の張り合わせディスクの場合を示している。両者は、レーザトリミングを行う上で、基本的には、同じ工程（５）（６）で処理されるが、主なる相違点を簡単に説明する。まず、１層式の場合は、反射層が７０％以上の高反射率を有するアルミの膜であるのに対して、２層式の場合は、読みとり側の基板８０１に形成される反射層８０１が、３０％の反射率を有する半透過性の金（Ａｕ）の膜であり、印刷層側の基板８０３に形成される反射層８０２は、上記１層式の場合と同じものである。次に、２層式の場合は、１層式に比べて、接着層８０４が、光学的に透明であること、厚みが均一であること、レーザトリミングにより光学的な透明性を失わないこと等の光学的な精密度が要求される。又、第７図（７）、（８）、（９）では２層の記録層のディスクの第１層の波形を示す。２層目の波形そのものは１層目の波形に比べて単に信号レベルが低いだけでさほど変わらない。しかし、１層と２層は張り合わせてあるため両者の相対位置精度はランダムであり数百ミクロンの精度でしか制御できない。後で説明するが、レーザービームは２枚の反射膜を貫通しているため、海賊版ディスクをつくるには、例えば第１マークの１層目の位置情報と２層目の位置情報を正規ディスクと同じ値に一致させる必要がある。しかし一致させるには、サブミクロンに近い張り合わせ精度が必要であるため、２層方式の海賊版ディスクの製造は事実上不可能となる。

ここで、この光学マーキング無反射部作成技術について、以下の（ａ）～（ｄ）で、張り合わせタイプと単板タイプについて、更に詳しく、第８図～第１２図等

を参照しながら説明する。第８図（ａ），（ｂ）は、光学マーキング無反射部を平面的に見た場合の顕微鏡写真であり、第１０図は、２層式の張り合わせディスクの無反射部の略示断面模式図である。

（ａ）５μｊ／パルスのＹＡＧレーザーを用いて０．６ｍｍ厚のディスクを張り合わせた合計１．２ｍｍ厚のＲＯＭディスクの０．６ミリの深さにある５００オングストロームのアルミ層にレーザーを照射したところ、第８図（ａ）の７５０倍の顕微鏡写真に示すような１２μｍ幅のスリット状の無反射部８１５が形成された。この場合、７５０倍の顕微鏡写真では、無反射部８１５には、アルミの残りカスは全く確認できなかった。無反射部８１５と反射部との境界部には２０００オングストロームの厚みで、２μｍ幅の厚く盛り上がったアルミ層が観察できた。第１０図（ａ）に示すように内部では大きな破損が起こっていないことを確認した。この場合、パルスレーザーの照射によりアルミの反射層が溶融し、表面張力により両側の境界部に蓄積される現象がおこっていると考えられる。我々は、これをＨＭＳＴ記録方式と呼ぶ（Hot Melt Surface Tention Recording Method）。この現象は貼り合わせディスク８００にのみ観察される特徴的な現象である。更に、第１１図に、上記レーザートリミングによる無反射部の断面を、透過電子顕微鏡（ＴＥＭ）により観察した結果を基にした模式図を示す。尚、同図によれば、アルミの膜厚増大部の巾方向領域を１．３μｍ、厚みを０．２０μｍとすると、その部位での増大アルミの量は、１．３×（０．２０－０．０５）＝０．１９５μm^2となる。レーザー照射部領域（１０μｍ）の半分の領域（５μｍ）にあったアルミの量は、５×０．０５＝０．２５０μm^2となる。従って、それらの差を計算すると、０．２５０－０．１９５＝０．０５５μm^2となる。これを長さに、換算すると、０．０５５／０．０５＝１．１μｍとなる。このことか

ら、厚みが０．０５μｍのアルミ層が１．１μｍの長さだけ残留していることになり、事実上、レーザー照射部のアルミはほぼ全部、膜厚増大部に引き寄せられたと考えてよい。このように、同図による解析の結果からも、上記特徴的な現象についての説明が正しいことが分かる。

（ｂ）次に、単板の光ディスク（１枚のディスクにより構成される光ディスク）の場合について説明する。片面の成形ディスクの０．０５μｍ厚のアルミの反射膜に同じパワーのレーザパルスを加えた場合の実験結果を第８図（ｂ）に示す。図に示されているようにアルミの残査が残っており、このアルミ残査が再生ノイズになるため、高い密度とエラーの少なさが要求される光ディスクの情報の２次記録用途には適していないことがわかる。又、貼り合わせと異なり第１０図（ｂ）に示すように単板ディスクの場合、無反射部がレーザートリミングされる時、必ず保護層８６２が破損する。破損の程度はレーザーパワーにより様々であるが、レーザーパワーを精密に制御しても破損はさけられない。さらに我々の実験では保護層８６２の上に数百μｍの厚さでスクリーン印刷された印刷層８０５が熱吸収率の大きい場合破損された。単板の場合、保護層の破損に対処するため、保護層をもう一度塗布するか保護層を塗布する前にレーザーカットすることが必要となる。いずれにしても単板方式ではレーザーカット工程がプレス工程の中に限定されるという課題が予想される。従って単板ディスクの場合、有効度は高いが、用途が限定される。

（ｃ）以上は、２層式の張り合わせディスクを用いて、単板のディスクと張り合わせディスクとの比較を説明した。上記説明からわかるように、１層式の張り合せたディスクの場合でも、２層式の場合と同様の効果が得られる。従って、ここでは、第１２図（ａ）、（ｂ）等を用いて、１層式の場合について、更に説明

する。第１２図（ａ）に示すように反射層８０２の一方は、ポリカからなる透明基板８０１で、もう一方は硬化した状態の接着層８０４と基板により充填された密閉状態となっている。この状態で、パルスレーザーを集束させ加熱すると、反射層８０２に本実験の場合７０ｎｓの短い時間に５μＪ／パルスの熱が１０～２０μｍの直径の円形のスポットに加わる。このため瞬時に融点である６００℃に達し溶融状態になる。熱伝導により近接した透明基板８０１のごく一部が溶け、接着層８０４も一部が溶ける。第１２図（ｂ）に示すようにこの状態で溶融したアルミは表面張力により、両側に張力が加わるため、溶けたアルミは境界部８２１ａ、８２１ｂに集まり、集中部８２２ａ、８２２ｂが形成され再び固まる。こうしてアルミの残査のない無反射部５８４が形成される。よって、第１０図（ａ）に示すように貼り合わせディスクにすることにより、レーザートリミングした場合はっきりとした無反射部５８４が得られる。単板の場合に発生する保護膜の破壊による外部環境への反射層の露出は、レーザーパワーを最適値より１０倍以上上げてもみられなかった。レーザートリミングの後、第１２図（ｂ）に示すように無反射部５８４は２枚の透明基板８０１によりサンドウィッチ構造になるとともに両側が接着層８０４により、外部の環境から遮断されているため環境の影響から保護されるという効果がある。

（ｄ）さらに、ディスクを２枚張り合わせることによる、他の利点について、説明する。バーコードで二次記録した場合、第１０図（ｂ）に示すように、単板ディスクでは不正業者が、保護層を除去することによりアルミ層を露出させられる。このため、正規ディスクのバーコード部にアルミ層を再度蒸着し、再度別のバーコードをレーザートリミングすることにより、暗号化されていないデータ部を改ざんされる可能性がある。例えば、ID番号を平文、もしくは主暗号と分離して記

録した場合、単板では改ざんされ、他のパスワードでソフトの不正使用が行われる可能性がある。しかし、第１０図（a）のように貼り合わせディスク
に二次記録した場合、貼り合わせディスクを２枚にはがすのは困難である。このことに加えて、はがす時にアルミ反射膜が部分的に破壊される。海賊版防止マーキングが破壊された場合、海賊版ディスクと判別され、作動しなくなる。従って、貼り合わせディスクの場合不正改ざんした場合の歩留りが悪くなり、経済的に不正改ざんが抑制される。特に、２層式の貼り合わせディスクの場合、ポリカ材料は温度湿度の膨張係数をもつため、一旦はがした２枚のディスクの１層と２層の海賊版防止マーキングを数μmの精度で貼り合わせて量産することは不可能に近い。従って、２層の場合、さらに防止効果は高くなる。こうして張り合わせディスク８００にレーザートリミングすることにより鮮明な無反射部５８４のスリットが得られることが明らかになった。

以上の説明（ａ）～（ｄ）で、光学マーキング無反射部の作成技術に関して説明した。

（Ｃ）次に、作成されたマーキング位置の読み取り工程を説明する。

第１５図は、光ディスクの製作過程における、光学マーキング無反射部を検出するための低反射光量検出部５８６を中心としたブロック部である。又、第１６図は、低反射部のアドレス・クロック位置検出の原理図である。尚、以下の説明では、便宜上、１枚のディスクから構成された光ディスク上の無反射部を読み取り対象とした場合の動作原理について説明する。この動作原理は、２枚のディスクを張り合わせた光ディスクの場合にも勿論当てはまる。

第１５図に示すように、ディスク８００を低反射部位置検出部６００を有するマーキング読み取り装置に装着し、マーキングを読み取った場合、ピットの有無

による信号波型８２３と無反射部５８４の存在による信号波型８２４は信号レベルが大きく異なるため、簡単な構成の回路で、第９図（ａ）の波形図に示すように明確に区別できる。

この波形をもつ無反射部５６４の開始位置と終了位置は、第１５図のブロック図の低反射光量検出部５８６によって容易に検出される。そして、再生クロック信号を基準信号とすることにより、低反射部位置情報出力部５９６において位置情報が得られる。

第１５図に示すように、低反射光量検出部５８６の比較器５８７は光基準値５８８より低い信号レベルのアナログの光再生信号を検出することにより、低反射光量部を検出する。検出期間中、第１６図の（5）のような波形の低反射部検出信号を出力する。この信号の開始位置と終了位置のアドレスとクロック位置を測定する。

さて、光再生信号は、ＡＧＣ５９０ａをもつ波形整形回路５９０により、波形整形されデジタル信号となる。クロック再生部３８ａは波形整形信号より、クロック信号を再生する。復調部５９１の、ＥＦＭ復調器５９２は信号を復調し、ＥＣＣは誤り訂正し、デジタル信号が出力される。ＥＦＭ復調信号は物理アドレス出力部５９３において、ＣＤの場合サブコードのＱビットからＭＳＦのアドレスがアドレス出力部５９４から出力され、クレーム同期信号等の同期信号が同期信号出力部５９５より出力される。クロック再生部３８ａからは復調クロックが出力される。

低反射部アドレス／クロック信号位置信号出力部５９６においては、ｎ－１アドレス出力部５９７とアドレス信号、そしてクロックカウンター５９８と同期クロック信号もしくは復調クロックを用いて、低反射部開始／終了位置検出部５９

９により低反射部５８４の開始点と終了点を正確に計測する。この方法を第１６図の波形図を用いて具体的に説明する。第１６図の（１）の光ディスクの断面図のように、マーク番号１の低反射部５８４が部分的に設けられている。第１６図（２）のような反射信号つまり第１６図（３）のようなエンベロープ信号が出力され、反射部において、光量基準値５８８より低くなる。これを光量レベル比較器５８７により検出し、第１６図（５）のような低反射光量検出信号が低反射光量検出部５８６から出力される。又、第１６図（４）の再生デジタル信号に示すように、マーク領域は反射層がないため、デジタル信号は出力されない。

次に、この低反射光量検知信号の開始、終了位置を求めるためには、アドレス情報と第１６図（６）の復調クロックもしくは同期クロックを用いる。まず、第１６図（７）のアドレスｎの基準クロック６０５を測定する。ｎ－１アドレス出力部５９７により、予め、アドレスｎの一つ前のアドレスを検知すると、次のｓｙｎｃ６０４はアドレスｎのＳｙｎｃであることがわかる。このｓｙｎｃ６０４と低反射光量検知信号の開始点つまり基準クロック６０５までのクロック数をクロックカウンター５９８でカウントする。このクロック数を基準遅延時間ＴＤと定義し、基準遅延時間ＴＤ測定部６０８が測定し、記憶する。

読み取り用再生装置により、回路の遅延時間が異なるためこの基準遅延時間ＴＤは読み取り用再生装置により異なる。そこで、このＴＤを用いて時間遅れ補正部６０７が時間補正を行うことにより、設計の異なる読み取り用再生装置においても低反射部の開始クロック数が正確に測定できるという効果がある。次に第１６図（８）のように次のトラックの光学マークＮｏ．１に対する開始、終了アドレス・クロック数を求めるとアドレスｎ＋１２のクロックｍ＋１４が得られる。ＴＤ＝ｍ＋２であるから、クロック数は１２に補正されるが説明ではｎ＋１４を

用いる。この読み取り用再生装置により、基準遅延時間ＴＤを求めなくとも、ばらつく遅延時間の影響をなくすもう一つの方法を述べる。この方法は、第１６図(8)のアドレスnのマーク１ともう一つのマーク２の相対的な位置関係が一致しているかを照合することにより、正規ディスクかどうかを判別できる。つまり、ＴＤを変数として無視し、測定したマーク１の位置A1＝a1＋ＴＤとマーク２の位置A2＝a2＋ＴＤの差を求めるとA1－A2＝a1－a2となる。同時に暗号を復号したマーク１の位置a1とマーク２の位置情報a2の差a1－a2と一致するかを照合することにより正規ディスクかどうかを照合できる。この方式であるとより簡単な構成で基準遅延時間ＴＤのバラつきを補正した上で位置を照合できるという効果がある。

（Ｄ）つぎに暗号書き込み工程を説明する。（Ｃ）において読み取られた位置情報は、後の（２）で詳しく述べるようにして暗号化（ディジタル署名化）され、バーコード等の方法で、光ディスクに書き込まれる。その様子を示すのが、第３図である。即ち、第３図（１）においてパルスレーザーにより、反射層がトリミングされ、同図（２）のようなバーコード状のトリミングパターンが形成される。再生装置側（プレーヤ側）では同図（３）のように、波形が部分的に欠落したエンベロープ波形が得られる。欠落部は通常のピットによる信号では発生しない低いレベルの信号を生じさせるので、これを第２スライスレベルのコンパレータでスライスすると同図（４）のような低反射部の検出信号が得られる。同図（５）でこの低反射部検出信号からＰＷＭ復調部６２１により、暗号を含む信号が復調される。

以上は、光ディスク作成側の各種工程について説明した。次に、このようにして、完成した光ディスクをプレーヤ側で再生するための、再生装置（プレーヤ）について、第４１図を用いてその構成と動作を併せて説明する。

同図において、最初に光ディスク９１０２の構成を説明する。光ディスク９１０２に形成された反射膜（図示省略）には、マーキング９１０３が施されている。そのマーキング９１０３の位置が、光ディスクの製造段階において、位置検出手段によって検出され、その検出された位置がマーキングの位置情報として光ディスクに暗号化されて、バーコード９１０４で書き込まれている。

位置情報読み取り手段９１０１は、そのバーコード９１０４を読み取って、内蔵する復号化手段９１０５によって、そのバーコードの内容を復号化して出力する。マーキング読み取り手段９１０６は、マーキング９１０３の現実の位置を読み取って、出力する。比較判定手段９１０７は、位置情報読み取り手段９１０１に内蔵された復号手段９１０５による復号結果と、マーキング読み取り手段９１０６による読み取り結果とを比較し、両者が所定の許容範囲内で一致しているか否かを判定する。一致している場合は、光ディスクを再生するための再生信号９１０８を出力し、一致していなければ、再生停止信号９１０９を出力する。制御手段（図示省略）は、それらの信号に従って、光ディスクの再生動作を制御し、再生停止信号が出された場合は、不正に複製された光ディスクである旨の表示を表示部（図示省略）に行って、再生動作を停止させる。ここで、マーキング読み取り手段９１０６は、マーキング９１０３の現実の位置を読み取る際に、復号化手段９１０５の復号結果を利用してももちろんよい。

この様な再生装置によれば、不正に複製された光ディスクを検知して、その再生を停止することが出来、事実上不正な複製を防止出来る。

ここで、光ディスクの製造からプレーヤ側の再生についての説明を終えて、それらの内容に関連する、付随的事項について説明する。

（A）低反射部の位置情報リストである低反射部アドレス表について説明する。

（ａ）即ち、予め工場において、海賊版防止マーク作成工程により、無作為にレーザーマーキングを形成する。この様にして、形成されたレーザーマーキングは、同じ形状のものは作れない。次の工程では各ディスク毎に低反射部５８４を上述したようにしてＤＶＤの場合、０．１３μｍの分解能で測定し、第１３図（ａ）に示すような低反射部アドレス表６０９を作成する。ここで、第１３図（ａ）は、本実施例により作成される正規のＣＤの低反射部アドレス表などを表した図であり、第１３図（ｂ）は、ＣＤが不正複製されたものである場合の図である。この低反射部アドレス表６０９を第１８図に示すような一方向関数で暗号化し、第２図に示すように、ディスクを最内周部に、バーコード状の反射層のない低反射部群５８４ｃ～５８４ｅを、２回目の反射層形成工程において、記録する。もしくは第１４図に示すように、ＣＤ－ＲＯＭの磁気記録部６７に記録してもよい。第１８図は、暗号化に用いる一方向関数によるディスク照合のフローチャートであり、第１４図は、ディスク作成装置、及び専用の記録再生装置のブロック図である。第１３図に示すように正規のＣＤと不法に複製されたＣＤでは低反射部アドレス表６０９、６０９ｘが大幅に異なる。その要因の１つは、上述したように、レーザーマーキングは、同じ形状のものが作れないからである。更に、ディスクにおいて予め割り当てられたセクタのアドレスが、ディスクの原盤相互間で相違することも両者が大幅に異なる第２の要因である。

即ち、ここで、第１３図を参照しながら、マーキングに関して、正規ディスクと海賊版ディスクとで得られる位置情報の違いを説明する。同図では、上記第１、第２の要因が重なっている場合である。又、マーキングは、ディスク上に２つ形成されている。即ち、マーク番号１のマーキングに対して、正規のＣＤの場合、アドレス表６０９に示されているように第１マークは、論理アドレスＡ１のセク

タの中の開始点より２６２番目のクロックの位置にある。１クロックはＤＶＤの場合、０．１３μｍであるため、この精度で測定されている。次に、海賊版ＣＤの場合、アドレス表６０９ｘに示されているように、アドレスＡ２のセクタの中の８１番目のクロックの位置にある。このように、第１マークの位置が正規ディスクと海賊版ディスクでは違うことから海賊版ディスクを発見することができる。同様に、第２マークの位置も異なる。この正規ディスクと位置情報を一致させるには、アドレスＡ１のセクタの２６２番目の位置の反射膜を１クロック単位つまり、０．１３μｍの精度で加工しないと海賊版ディスクは作動しない。

従って第１４図のように、再生装置においてこの暗号化された表を復号して、正規の表をつくり、照合プログラム５３５により照合することにより、正規のディスクと不法複製されたディスクを区別することができ、複製ディスクの動作を停止できる。第１６図の例では第１７図に示すように正規のディスクと不正複製されたディスクでは低反射部アドレス表６０９、６０９ｘの値が異なる。第１６図（8）のように正規ディスクではマーク１の次のトラックでは開始終了はｍ＋１４、ｍ＋２６７であるが、第１６図（9）のように不法複製されたディスクではｍ＋２１、ｍ＋２７７となり異なる。こうして第１７図に示すように低反射部アドレス表６０９、６０９ｘの値が異なり複製ディスクを判別できる。この低反射部アドレス表６０９をもつディスクを不法複製業者が複製する場合は、彼らは第１６図（8）に示すように再生クロック信号の分解能で正確にレーザートリミングを行う必要がある。DVDディスクの場合、第２７図（5）に示すように再生クロックパルスの周期Tをディスク上の距離に換算した場合0.13μmになる。従って、不法複製するには0.1μmのサブミクロンの分解能で反射膜を除去することが要求される。確かに光ディスク用の光ヘッドを用いた場合、サブミクロンの精度でCD

-Rのような記録膜に記録できる。しかし、この再生波形は第９図（c）のようになり、第９図（a）のような特異な波形824は反射膜を除去しない限り得られない。

（b）従ってこの反射膜をとり除く海賊版の量産方法としてはYAG等の大出力レーザーを用いたレーザートリミングが１番目の方法として考えられる。現状では最も精度の高い工作用レーザートリミングの加工精度は数μmしか得られない。半導体のマスク修正用レーザートリミングにおいても１μmが加工精度の限界であるといわれている。つまり、レーザートリミングでは0.1μmの加工精度を量産レベルで達成することは難しい。

（c）二番目の方法として、現在サブミクロンの加工精度を達成しているのは、超LSIの半導体マスクの加工用のX線露光装置やイオンビーム加工装置が知られているが、非常に高額な装置で１枚あたりの加工時間も要するため、ディスク１枚毎に加工すると１枚のコストは高額なものとなる。従って、現行では殆どの正規ディスクの販売価格を上回るコストとなり、採算がとれなくなり、海賊版ディスクを作る意味がなくなってしまう。

（d）以上のように第１の方法であるレーザートリミングでは、サブミクロン加工が困難なため、海賊版ディスクの量産が困難である。又、第２の方法であるX線露光等のサブミクロン加工技術では、１枚あたりのコストがかかりすぎて、経済面で海賊版ディスクの生産が無意味となる。従って、低コストのサブミクロンの量産加工技術が実用化されるのまでの間、海賊版の複製は防止される。このような技術が実用化されるのは遠い将来のことであるので海賊版の生産は防止される。また２層ディスクの各層に低反射部を設けた場合、第３３図に示すように上下のピットを合わせて精度よく貼りあわせないと海賊版ディスクは複製できないため、防止効果はさらに上がる。

（B）次に、低反射部のディスク上の配置角度を所定のように特定する事項について説明する。

本発明では、反射層レベルつまり低反射部マーキングだけで充分な海賊版防止効果がある。この場合、原盤は複製品であっても防止効果がある。しかし、原盤レベルの海賊版防止技術と組み合わせることにより、さらに防止効果を高められる。低反射部のディスク上の配置角度を第１３図（a）の表５３２ａと表６０９のように特定すると、海賊版業者は原盤の各ピットの配置角度の状態まで正確に複製する必要がある。海賊版のコストが上がるため、抑制効果がさらに上がる。

（C）次に、ここで本発明のポイントをまとめる。本発明では正規業者は数十μｍの加工精度の汎用のレーザートリミング装置で加工すれば、正規のディスクが作れる。測定精度には０．１３μｍが要求されるが、これは民生用のＤＶＤプレーヤーの一般的な回路で測定できる。この測定結果を暗号の秘密鍵で暗号化することにより正規ディスクが生産できる。つまり、正規業者は秘密鍵と０．１３μｍの測定精度の測定器のみが要求され、要求される加工精度は２～３桁悪い数十μｍである。従って、一般のレーザ加工装置でよい。一方、海賊版業者は、秘密鍵をもっていないため、正規ディスクの暗号をそのままコピーせざるを得ない。この暗号の位置情報つまり、正規ディスクの位置情報に対応した物理マークを０．１３μｍの加工精度で加工する必要がある。つまり正規業者の加工機より２桁高い加工精度の加工機で低反射部マークを作成する必要がある。この２桁高い加工精度つまり、０．１μｍの精度による量産は技術的にも経済的にも近い将来を考えても困難である。このため、海賊版ディスクはＤＶＤ規格存続中は防止されることになる。つまり、本発明の一つのポイントは一般的に測定精度が加工精度より数桁高いことを利用している点にある。

以上のことはＣＬＶの場合、前述のように原盤のアドレスの座標配置が異なることを利用している。第１９図に実際のＣＤのアドレスの位置について測定した結果を示す。一般に、ディスク原盤は、一定回転数つまり等角速度（ＣＡＶ）でモーターを回転させて記録されたものと、一定の線速度つまり等線速度（ＣＬＶ）でディスクを回転させて記録されたものの２種類がある。ＣＡＶディスクの場合、論理アドレスは所定の角度上に配置されるため、論理アドレスと原盤上の物理的配置角度は何度原盤を作成しても全く同じである。しかし、ＣＬＶディスクの場合、線速度しか制御しないため、論理アドレスの原盤上の配置角度はランダムになる。第１９図の実際のＣＤの論理アドレスの配置測定結果に示すように、全く同じデータを原盤作成装置で記録しても、トラッキングピッチや開始点や線速度が毎回微妙に違い、この誤差が累積されるため、物理的配置が異なる。第１９図では、第１回目に作成した原盤の各論理アドレスのディスク上の配置を白丸で示し、第２回目、第３回目に作成して原盤の配置を黒丸、三角で示す。このように原盤を作成する毎に論理アドレスの物理配置がことなることがわかる。尚、第１７図は、正規のディスクと不正複製されたディスクの低反射部アドレス表の比較図である。

以上、原盤レベルの防止方式を述べた。これは、同じ論理データから原盤作成装置を用いてＣＤやＤＶＤのようなＣＬＶ記録の原盤を作成した場合、第１９図に示すように、正規ディスクと海賊版ディスクでは、各ピットの原盤上の物理的配置が原盤毎に異なる。この点に着目して正規ディスクと海賊版ディスクの識別を行うものである。原盤レベルの海賊版防止技術は単純に正規ディスクのデータのみを複写した論理レベルの海賊版を防止できる。しかし、最近ではより高度の技術をもつ海賊版業者が登場し、正規ディスクのポリカ基板を溶かすことにより、

正規ディスクと全く同じ物理形状のレプリカの原盤を作成することが可能となっている。この場合、原盤レベルの海賊版防止方式は破られてしまう。この新たな海賊版ディスクの生産を防止するため、本発明では反射膜にマーキングする反射層レベルの海賊版防止方式を考案した。

さらに、本発明の方法では、上述のように、例え原盤が同じでも、原盤を用いて成形されたディスク一枚毎に反射膜作成工程で反射膜を一部削除することによりマーキングを作成する。従って、ディスク毎に低反射部マーキングの位置や形状が異なる。サブミクロンの精度で正確に反射膜を部分的に削除することは、通常工程では不可能に近い。従って本発明のディスクを複製することは経済的に成立しないため、複製防止の効果は高い。

尚、第２０図に低反射部アドレス表による複製ＣＤの検出フローチャート図を示す。再生装置の光ヘッドや回路等の設計により、光マークの検出に要する遅延時間が、ごくわずかであるが異なる。この回路遅延時間ＴＤは設計時点もしくは量産時点で、予測できる。光マークはフレーム同期信号からのクロック数つまり時間を測定して位置情報を得る。このためこの回路遅延時間の影響により、光マークの位置情報の検出データに誤差が生じる。すると正規のディスクまで海賊版ディスクであると判定してしまい正規の使用者に迷惑を与える。そこで、回路遅延時間ＴＤの影響を軽減する工夫を述べる。又、ディスクの購入後についた傷により、再生クロック信号が途切れるため光マークの位置情報の測定値に数クロックの誤差が生じることから、これについての対策として、ディスクに第２７図の許容誤差８６６と合格回数８６７を記録し、再生時における測定値の許容誤差を実状に応じて認めるとともに、合格回数８６７に達した時点で、再生を許可することによりディスクの表面の傷による誤差の許容範囲をディスクの出荷時に著作

権者がコントロールできる工夫を第２０図を用いて説明する。

即ち、第２０図において、ステップ８６５ａでディスクを再生して、本発明のバーコード記録部もしくはピット記録部より暗号化された位置情報を入手する。ステップ８６５ｂで復号もしくは署名検証を行い、ステップ８６５ｃで光マークの位置情報リストを得る。次に再生回路の遅延時間ＴＤが再生装置の第１５図の回路遅延時間記憶部６０８ａの中に入っている場合はステップ８６５ｈより、ＴＤを読み出し、ステップ８６５ｘへ進む。ＴＤが再生装置にない時、もしくはディスクに測定命令が記録されている時は、ステップ８６５ｄに進み基準遅延時間の測定ルーチンに入る。アドレスＮｓ－１を検知すると次のアドレスＮｓの開始位置がわかる。フレーム同期信号と再生クロックをカウントし、ステップ８６５ｆで基準の光マークを検知する。ステップ８６５ｇで回路遅延時間ＴＤを測定し、記憶する。なお、この動作は第１６図（７）を用いて後述する動作と同じである。ステップ８６５ｘでアドレスＮｍの中にある光マークを測定する。ステップ８６５ｉ，８６５ｊ，８６５ｋ，８６５ｍにおいてはステップ８６５ｄ，８６５ｙ，８６５ｆ，８６５ｙと同様にして、光マークの位置情報をクロック単位の分解能で検出する。次にステップ８６５ｎで、海賊版ディスクの検知ルーチンに入る。まず、回路遅延時間ＴＤを補正する。ステップ８６５ｐで、第２７図に示すディスクに記録されている許容誤差８６６つまりｔＡと合格回数８６７を読み出し、ステップ８６５ｇで測定した位置情報が許容誤差ｔＡの範囲に収まっているかを照合する。ステップ８６５ｒでこの結果がＯＫなら、ステップ８６５ｓで、照合したマーク数が合格回数に達したかをチェックし、ＯＫならステップ865uで正規ディスクと判別し、再生を許可する。まだ、合格回数に達していない場合はステップ８６５ｚへ戻る。ステップ８６５ｒでＮＯの場合は、ステップ８６５ｆで誤

検出回数がＮＡより少ないかをチェックしＯＫの場合のみ、ステップ８６５ｓへ戻る。ＯＫでない時は、ステップ８６５ｖで不正ディスクと判定して停止する。

以上のようにして、再生装置の回路遅延時間ＴＤをＩＣのＲＯＭ内に記録してあるので、より正確に光マークの位置情報が得られる。又、ディスクのソフト毎に許容誤差８６６と合格回数を設定することにより購入後のディスクについた傷に対して、実態に合わせて海賊版ディスクの判定基準を変更できるので、正規ディスクを誤判別する確率が低くなるという効果がある。

（Ｄ）ここで、２枚のディスクを張り合わせた光ディスクにおける光学マーキング無反射部の読み取りに関する説明における、上記動作原理では、触れなかった点を中心として述べる。

即ち、第１６図のように開始位置のアドレス番号、フレーム番号、クロック番号が１Ｔ単位の分解能つまり、ＤＶＤ規格においては一般プレーヤーで０．１３μｍの分解能で本発明の光学マークを正確に測定できる。第１６図の光学マークのアドレスの読みとり方法をＤＶＤ規格に適用したものを第２７図と第２８図に示す。第１６図と同じ動作原理であるため第２７図、第２８図の信号（１）（２）（３）（４）（５）の説明は省略する。

ここで、CDの場合の低反射部の位置検出原理図である第１６図と、DVDの場合の第２７図、第２８図との対応について述べる。

第１６図（5）は、第２７図（1）、第２８図（1）に対応する。第１６図（6）の再生クロック信号は、第２７図（5）、第２８図（5）に対応する。第１６図（7）のアドレス603は、第２７図（2）、第２８図（2）に対応する。

第１６図（7）のフレームSync604は、第２７図（4）、第２８図（4）に対応する。第１６図（8）の開始クロック番号605aは、第２７図（6）の再生チャンネル

クロック番号に対応する。第１６図（7）の終了クロック番号606に代えて、第２７図（7）、第２８図（7）では6bitのマーキング長を用いてデータの圧縮を計っている。

図示するようにCDとDVDでは基本的に検出動作は同じであるが、第１の違いとして第２７図（7）の1bitのマークの層識別子に603aに示すように、低反射部が１層であるか、２層であるかの識別子が入っている点が異なる。DVDの２層の場合、上述のように防止効果が高まる。第２の違いとして線記録密度が倍近く高いため、再生クロックの1Tが0.13μmと短くなり、より位置情報の検出分解能が上がり、防止効果が高い。

第２７図の場合、２層の反射層をもつ２層式の光ディスクを用いた場合の一層目の信号を示し、信号（１）は１層目の光学マークの開始位置を検出した状態を示す。第２８図は２層目の信号の状態を示す。

２層目を読み出す時は、第１５図の１層２層部切換部８２７より焦点制御部８２８に切り換え信号を送り１層から２層へ焦点駆動部８２９により焦点を切り換える。第２７図からアドレス（n）であることがわかり、信号（４）のフレーム同期信号をカウンタでカウントすることにより、フレーム４にあることがわかる。信号（５）のＰＬＬ再生クロック番号がわかり、信号（６）の光学マーキング位置データが得られる。この位置データを用いて、一般の民生用ＤＶＤプレーヤで光学マークを０．１３μmの分解能で測定することができる。

（E）次に、２枚のディスクを張り合わせた光ディスクのさらに関連事項を説明する。

第２８図は、２層目にできた光マーキングのアドレス位置情報を示す。第７図の工程（b）で示したように、レーザー光は１層、２層を貫通させて同じ穴で開

けるため、第１層の反射層８０２にできた無反射部８１５と第２反射層８２５にできた無反射部８２６とは同じ形状をしている。この状態を第３３図に表わした斜視図で示す。本発明では透明基板８０１と第２基板８０３を張り合わせた後にレーザを貫通させて２層に同じマークを作成する。この場合、１層と２層はピットの座標配置が異なることと、貼り合わせ時の１層、２層間の位置関係はランダムであるため、１層と２層では各々異なるピット部にマークが形成され、全く異なる位置情報が得られる。この２つの位置情報を暗号化して海賊版防止ディスクを作成する。このディスクを不正に複製しようとした場合、各々２層の光学マークを０．１３μｍ程度の精度で一致させる必要がある。前述のように０．１３μｍつまり０．１μｍの精度で光マークで光マークとピットを一致させて複製することは現状では無理であるが、将来、低コストで０．１μｍの加工精度で１層ディスクを大量にトリミングできる量産技術が実現する可能性はある。この場合でも２層貼り合わせディスク８００の場合、上下２枚のディスクが同時トリミングされるので、上下２枚のピット配置および光学マークを数μｍの精度で合わせる必要がある。しかし、ポリカ基板の温度係数等によりこの精度で張り合わせることは、不可能に近い。このため２層のディスク８００にレーザーを貫通させ光学マークを作成した場合、複製が著しく困難な海賊版防止マークが得られる。このため海賊版防止効果が高くなるという効果が得られる。以上のようにして、海賊版防止処理が施された光ディスクが完成する。この場合、海賊版防止用途の場合、単板のようにディスク工程とレーザーカット工程が分離できない場合、レーザーカット工程と一体となった暗号化工程及び暗号の秘密鍵の処理はディスク工場の中で行うことになる。つまり、単板方式はソフト会社のもつ暗号用の秘密鍵をディスク工場に渡す必要があり、暗号の機密性が大幅に低下する。これに対し、本

発明の１つの対応である貼り合わせディスクにレーザー加工する方式はレーザートリミングがディスク製造工程とは完全に分離できる。従って、ソフトメーカーの工場でもレーザートリミングと暗号化作業が行なえる。ディスク工場にソフトメーカーがもつ暗号の秘密鍵を渡す必要がなく、暗号の秘密鍵がソフトメーカーの外部に出ないため、暗号の機密性が大幅に向上する。

（２）次に、上述したように、（１）において簡単に述べられた、（Ａ）マーキング位置情報等の暗号化（ディジタル署名）等、光ディスクの位置情報等復号再生等について詳細に説明する。又、（Ｂ）その他の、海賊版防止に関する様々な工夫についても述べる。

（Ａ）暗号化（ディジタル署名）とその再生について説明する。

（ａ）単純な暗号化（ディジタル署名）の場合：

（ＲＳＡ関数を用いた場合の説明）

先ず、暗号化を行う際に利用する関数として、ＲＳＡ関数のようなメッセージリカバリー型署名方式の関数を用いて暗号化する場合の例を、第２２図、第２４図に示すフローチャートを参照しながら説明する。

第２２図に示すように、大きなルーチンとしては、光ディスクメーカ側における、マーキングの位置情報を測定するステップ７３５ａと、位置情報を暗号化（又は、署名）するステップ６９５と、再生装置側における、位置情報の復号化（又は、署名を検証あるいは認証）するステップ６９８と、正規の光ディスクかどうかの照合を行うステップ７３５ｗとから構成されている。

まず、ステップ７３５ａでは、ステップ７３５ｂで、光ディスク上のマーキングの位置情報を測定する。その位置情報をステップ７３５ｄで圧縮し、ステップ７３５ｅで圧縮した位置情報Ｈを得る。

ステップ６９５では、圧縮された位置情報Ｈの暗号を作成する。まず、ステップ６９５で、５１２ｂｉｔもしくは１０２４ｂｉｔのｄと、２５６ｂｉｔもしくは５１２ｂｉｔのｐとｑの秘密鍵を設定し、ステップ６９５ｂで、ＲＳＡ関数による暗号化を行う。位置情報Ｈを、図中に示したＭであるとすると、Ｍをｄ乗しｍｏｄ ｎの演算を行い暗号Ｃを得る。ステップ６９５ｄで暗号Ｃを光ディスク上に記録する。これにより、光ディスクが完成し、光ディスクの出荷が行われる（ステップ７３５ｋ）。

再生装置では、ステップ７３５ｍで光ディスクが装着され、ステップ６９８で暗号Ｃを復号する。具体的には、ステップ６９８ｅで暗号Ｃを再生し、ステップ６９８ｆで公開鍵としてのe,nを設定し、ステップ６９８ｂで暗号Ｃを復号するために、暗号Ｃをe乗し、更にその値のmod ｎを演算し平文Ｍを得る。この平文Ｍというのは、圧縮された位置情報Ｈである。尚、ステップ６９８ｇでエラーチェックを行ってもよい。エラーがない場合は位置情報が改ざんされてないと判断し、第２４図のディスクの照合ルーチン７３５ｗへ進む。エラーがある場合は正規のデータでないと判断して停止する。

さて、次のステップ７３６ａでは圧縮された位置情報Ｈを伸張し、元の位置情報が復元される。ステップ７３６ｃではの位置情報に示されている光ディスク上の位置に、実際にマーキングがあるかをどうかを測定する。ステップ７３６ｄでは、復号により得られた位置情報と、実際に測定した位置情報の差が許容範囲内かを照合する。ステップステップ７３６ｅでは、照合がOKならステップ７３６ｈへ進み、光ディスク内のソフトやデータの出力もしくはプログラムを動作させる。もし照合結果が許容範囲内にない場合、即ち双方の位置情報が一致しない場合は、不正に複製された光ディスクであると表示し、ステップ７３６ｇで停止させる。ＲＳ

Aの場合は、暗号だけを記録すればよいので、小さい容量でよいという効果がある。

(楕円関数を用いた場合の説明)

次に、暗号化を行う際に利用する関数として、別の方式であるインプリント型の署名方式の楕円関数を用いた場合の、第２３図、第２４図に示すフローチャートを参照しながら説明する。

第２３図等に示すように、大きなルーチンとしては、光ディスクメーカ側における、マーキングの位置情報を測定するステップ７３５ａと、その位置情報の認証暗号（すなわち署名）を演算するステップ７３５ｆと、再生装置側における、位置情報の認証（すなわち署名検証）を行うステップ７３５ｎと、正規の光ディスクであるかの照合を行うステップ７３５ｗとから構成されている。

まず、ステップ７３５ａから、ステップ７３５ｅまでは、ＲＳＡ関数の場合と同様である。

ステップ７３５ｆでは、圧縮された位置情報Ｈの認証暗号を作成する。まず、ステップ７３５ｇで、秘密鍵として、Ｘ（１２８ｂｉｔ以上）と、Ｋとを設定し、ステップ７３５ｈで、楕円曲線上の点で公開のシステムパラメータＧを決め、ｆ（ｘ）を一方向性関数（one direction function）とした場合、Ｒ＝ｆ（Ｋ×Ｇ）を求めた後、Ｒ’＝ｆ（Ｒ）を求め、Ｓ＝（Ｋ×Ｒ’－Ｈ）X^{-1}ｍｏｄＱの式により、認証暗号としてのＲ，Ｓを生成する。ステップ７３５ｊで認証暗号Ｒ，Ｓと、圧縮された位置情報の平文Ｈとを光ディスク上に記録し、ステップ７３５ｋでディスクを出荷する。

再生装置では、ステップ７３５ｍで光ディスクが装着され、ステップ７３５ｎで、位置情報の認証演算をおこなう。

まず、ステップ７３５ｐで装着された光ディスクから、認証暗号ＲとＳと、圧

縮された位置情報Hとを再生する。ステップ７３５ｒで、公開鍵Y、G、Qを設定し、ステップ７３５ｓで認証演算を行い、A＝SR^{-1}ｍｏｄQ、B＝HR^{-1}ｍｏｄQからｆ（A×Y＋B×G）を求め、ステップ７３５ｔで、この値がRと一致するかをチェックする。一致した場合は位置情報が改ざんされてないと判断し第２４図の光ディスクの照合ルーチン７３５ｗへ進む。一致していない場合は正規のデータでないと判断して停止する。

さて、次のステップ７３６aから、ステップ７３６ｇは、ＲＳＡ関数の場合と同様である。即ち、不正に複製された光ディスクであると判定した場合、その旨を表示し、ステップ７３６ｇで停止させる。尚、楕円関数の場合は、ＲＳＡ関数の場合と比べて、演算時間が短くて済むので、再生開始までの時間が短く出来るという効果があり、民生用の再生装置への応用に適している。

（ｂ）マスタ鍵とサブ鍵等を用いて、複雑に暗号化（ディジタル署名）する場合：

すなわち、マーキングの位置情報だけでなく、光ディスクに入力されるソフト内容の特徴情報や、海賊版防止識別子をも暗号化（ディジタル署名）の対象とし、さらに、マスタ鍵とサブ鍵の２つの暗号鍵をもつ点にある。尚、ここでの具体例としては、秘密鍵系暗号関数と公開鍵系暗号関数を併用した例を示す。

ここで、具体例の詳しい説明に入る前に、基本的な部分を理解するために、先ず第４０図を用いて、本例の基本的な構成を説明する。

尚、この基本的説明では、公開鍵系暗号関数により暗号化処理を行う場合の例であり、秘密鍵系暗号関数による暗号化処理は登場しない。そのため、公開鍵系暗号用のマスタ秘密鍵、公開鍵系暗号用のサブ秘密鍵は、それぞれ単にマスタ秘密鍵、サブ秘密鍵と呼ぶ。又、公開鍵系暗号用のマスタ公開鍵、公開鍵系暗号用

のサブ公開鍵は、それぞれ単にマスタ公開鍵、サブ公開鍵と呼ぶ。

第４０図に示すように、鍵管理センター９００１は、マスター秘密鍵をその秘密性が保たれる様に厳重に管理しており、後述するソフトメーカ９００２と通信回線９００３で結ばれている。そして、ソフトメーカ９００２から暗号化の依頼があった場合、ネットワーク９００３を介して送られた暗号化の対象を、そのマスター秘密鍵を用いて、暗号化する部門である。

ソフトメーカ９００２は、ここでは説明を単純にするために、ディスク工場をも含むものとする。従って、ソフトメーカ９００２は、ソフトの作成作業に加えて、第１図で述べたディスク工場での作業も行う部門である。即ち、映画のソフトを入力した光ディスクを製造する際に、海賊版業者の複製を防止するための暗号化の処理を併せて行う。この暗号化処理を実施するために、ソフトメーカ９００２は、鍵管理センタ９００１から、専用のサブ秘密鍵を渡されている。以上が、光ディスクのメーカ側の構成である。

一方、上記光ディスクを利用するユーザ側として、プレーヤ９００４がある。プレーヤ９００４は、光ディスクを再生するための装置であり、内蔵されたＲＯＭには、鍵管理センタが管理しているマスタ秘密鍵に対応したマスタ公開鍵があらかじめ格納されている。そして、不正に複製された光ディスクの再生を停止する機能を有している。

以上の様な構成において、次に動作説明を行う。

（ｂ－１）先ず、ソフトメーカ９００２が行う暗号化に関する工程を中心に述べる。

最初に行われる暗号化処理（第１暗号化処理）は、ディスクの金型を作る段階における暗号化であり、その暗号化された情報が、ディスクの金型の形状に反映

される。そして、最後に行われる暗号化処理（第２暗号化処理）は、レーザートリミングを行ってマーキングを作成した後の段階での暗号化である。

（１－１）第１暗号化処理では、第２暗号化処理の際に用いるサブ秘密鍵に対応するサブ公開鍵と、ソフト特徴情報と、海賊版防止識別子とを用いて暗号化し、その情報を通信回線９００３により鍵管理センタ９００１へ転送する。ここで、ソフト特徴情報とは、例えば、光ディスクに書き込む映画ソフトの内容を表した情報であり、各映画ソフトによって全て異なる固有の特徴情報である。又、海賊版防止識別子とは、製造された光ディスクが、海賊版防止の処理が施されたものであるか否かを検知出来るようにするためのものである。第２暗号を利用した海賊版防止の処理が施された光ディスクの識別子は”１”であり、その処理が施されていない場合は、”０”となる。本例では、この識別子は、当然、”１”となる。

（１－２）鍵管理センタ９００１は、ソフトメーカ９００２から転送されてきた上記情報を、自らが管理するマスタ秘密鍵を用いて暗号化して、それを再びソフトメーカ９００２へ返送する。このよにして生成された暗号を第１暗号と呼ぶ。

（１－３）ソフトメーカ９００２は、返送されてきた第１暗号を映画ソフト等と共に、ディスクの金型（又は、原盤）へ記録する。

（１－４）ソフトメーカ９００２は、このようにして製造した金型を使って、ディスクを成型する。

（１－５）次に、ソフトメーカ９００２は、成型したディスクを用いて光ディスクを作成して、上述した様にレーザートリミングを行い、光ディスク上にマーキングを形成する。

（１－６）更に、ソフトメーカ９００２は、そのマーキングの位置を検出して、

その検出の結果得られた位置情報を、自らが持っているサブ秘密鍵を用いて暗号化する。このようにして暗号化されたものを第２暗号と呼ぶ。この第２暗号は、位置情報を暗号化しているため、同じ金型から成型されたものであっても、１枚毎の光ディスクによって、全て異なるものであり、第１暗号と相違する点である。

（１－７）最後に、ソフトメーカ９００２は、この第２暗号を光ディスクにバーコードとして記録する。これにより光ディスクが完成する。

（ｂ－２）次に、この様にして完成された光ディスクを、ユーザが購入し、プレーヤ９００４を用いて再生する際の動作について説明する。

（２－１）先ず、プレーヤ９００４は、光ディスクに記録された第１暗号を読み出し、ＲＯＭに格納されているマスタ公開鍵を使って、第１暗号即ち、サブ秘密鍵に対応するサブ公開鍵と、ソフト特徴情報と、海賊版防止識別子とを合成して暗号化されたものを復号する。

（２－２）一方、プレーヤ９００４は、光ディスクに、現実に記録された映画ソフトの内容から、そのソフト特徴情報を抽出する。この抽出したソフト特徴情報と、（２－１）で、復号により得られたソフト特徴情報とを照合し、一致しなければ、不正に複製された光ディスクであるとの判断により、それ以降の再生動作を停止する。一致すれば、更に次に進む。

（２－３）即ち、（２－１）で、復号により得られた海賊版防止識別子が、”１”であるか、”０”であるかを調べる。”０”であれば、次に説明する処理を行わず、直ちに再生動作に入る。しかし、”１”であれば、更に、次に進む。

尚、これにより、第２暗号を利用した海賊版防止処理が、施されていない光ディスクであっても、正規に識別子が”０”に設定されている限り、プレーヤ９００４は、再生を行うものである。又、海賊業者が、この識別子が”０”となるよ

うにして、不正な複製を行おうとしても無理である。この識別子は、上述した様にソフト特徴情報などと共に合成されたのち、マスタ秘密鍵で暗号化されているからである。

（２－４）ここでは、先ず、光ディスクに記録されている第２暗号を読み出す。そして、その第２暗号即ち、位置情報を暗号化したものを、（２－１）で、復号により得られたサブ公開鍵を用いて復号する。

（２－５）復号された位置情報を用いて、その位置情報に対応する光ディスク上の位置に、実際にマーキングが存在するか否かを調べる。その結果、実際に測定されたマーキングの位置情報と、（２－４）で復号された位置情報とを照合する。不一致であれば、不正に複製された光ディスクであると判断して、再生動作を停止し、一致していれば、正規な光ディスクであると判断して、それ以降の再生を行う。

以上で、アウトラインの説明を終わり、次に、更に具体的な説明を行う。

即ち、第３２図に示すようにソフトコンテンツから各映像ソフトの各チャプターの時間構成を示すＴＯＣ情報や画像圧縮パラメータやタイトル名等の各々ソフトに固有なソフトパラメータをチェックサム演算とガロア体等の演算やＳＨＡやＭＤ５のような一方向性ハッシュ関数８６４ａにより１２８ｂｉｔから２５６ｂｉｔに圧縮したソフト特徴情報８６３を、ソフト特徴抽出手段８６４により抽出圧縮し、更にそれに加えて、各ソフトメーカー専門のサブ公開鍵８６１と、著作権識別子としての海賊版防止識別子８６５とを１つのデータに合成し、ステップ８６６ａ、８６６ｂで公開鍵系暗号のマスタ秘密鍵を用い、暗号化した上で、ステップ８６６ｅで原盤８６７に本体のソフトとともに記録する。

尚、秘密鍵系と、公開鍵系とを併用する方式を採用した場合は、ステップ８６

６ｃでは秘密鍵系暗号用マスタ秘密鍵を用い、ステップ８６６ｄで暗号化し、ステップ８６６ｅで原盤８６７に記憶する。

こうして原盤工程は完了する。原盤に記録した海賊版防止識別子８６５は、そのソフトが海賊版防止付かどうかを示すフラグが１ｂｉｔ、低反射部バーコード付かどうかを示すフラグが１ｂｉｔスクランブル付かどうかを示すスクランブル識別子９６５ａのフラグが１ｂｉｔ、ソフトのダビングを防止するかを示すフラグが１ｂｉｔ等の著作権保護フラグが４ｂｉｔ以上入っているもので、そのソフトが本来どのような著作権保護すべきかどうかを規定している。海賊版防止識別子８６５とサブ公開鍵８６１は、ソフト固有のソフト特徴情報８６３と合成されて公開鍵系暗号のマスタ秘密鍵により暗号化されているため改ざんできない。

海賊版防止識別子８６５とサブ公開鍵８６１は各ソフトに固有なソフト特徴情報８６３とともに１つのデータとして一括して秘密鍵により暗号化されている。

このソフト特徴情報８６３は２５６ｂｉｔとした場合、２の２５６乗の組み合わせがある。このため、ある特定の映画ソフトをオーサリングしたデータのソフト特徴情報を抽出した場合、他のソフトのソフト特徴情報と一致する確率は２の２５６乗分の１となり、まず一致することはない。ＭＤ５やＳＨＡの一方向性ハッシュ関数を用いた場合はハッシュ値、つまりソフト特徴情報９６３が２５６ｂｉｔの場合、現在得られる大型計算機を１０の１８乗年の間、演算しつづけないとハッシュ値が同じ２つのソフトコンテンツをみつけ出すことができないとされており、ソフトの入れ替えは困難となる。オーサリングした特定のソフトに対してソフト特徴情報は１つの値だけ存在し、かつ他のソフトと同じ値になることはない。

さて、特定のソフト特徴情報と海賊版防止識別子８６５とサブ公開鍵８６１は

一括して暗号処理されているため、この２つのどの値も変更することはできない。こうしてオーサリング後の特定のソフトに対する海賊版防止識別子８６５およびサブ公開鍵８６１は特定されることになる。

ここで、海賊版防止識別子８６５を原盤に記録する点について詳しく述べる。

各ソフトに対して、海賊版防止識別子８６５をどのように付与するかはソフトの著作権者の選択の問題である。光ディスクのソフトに海賊版防止対策を施すと、コストや手間がかかる。従って、全ての光ディスクに海賊版防止は施されず、海賊版防止もしくは本発明のバーコードのついた光ディスクとついていない光ディスクが混雑することになる。このように、海賊版防止やバーコードが付与されない正規ディスクも存在を認めると、当然再生装置はこれらのディスクを正常に再生する機能をもつ必要がある。この場合、ある海賊版対策なしディスクを再生する場合、そのソフトに対してソフト会社が正規に海賊版防止をはずした場合と、ソフト会社が海賊版防止機能付と定義したディスクのソフトを海賊版業者が海賊版防止識別子を不正に変更したものである場合の、２つのケースが考えられる。

従って、海賊版防止識別子が不正であるかを判別する手段が重要となる。

本発明では海賊版防止識別子を含む海賊版防止識別子８６５をソフト特徴情報とまとめて秘密鍵で暗号化し、原盤の暗号記録部に記録している。再生装置では所定の公開鍵で復号するので、いずれかを不正に変更することは防止される。

海賊版業者にできることは、ソフト特徴情報８６３と海賊版防止識別子８６５を含む第１暗号全部をそっくり入れ替えることだけである。

尚、このソフト特徴情報８６３を、後述する、現実に光ディスクに書き込まれた映画ソフトの中から抽出されるソフト特徴情報と区別するために、前者を第１のソフト特徴情報と呼び、後者を第２ソフト特徴情報と呼ぶこともある。両者は、

同じ映画ソフトの内容を対象としている点で同じであるが、前者は、光ディスク製造時に暗号化されて書き込まれ、後者は、再生時に現実に記録されている映画ソフトの内容を調べて、抽出される点で異なる。

第１ソフト特徴情報８６３はオーサリングの完了した各ソフトに固有の値であるため、別のソフトが同じ値になる確率は前述のように２の２５６乗分の１で殆どないといってよい。第１ソフト特徴情報８６３を入れ換えた場合、再生装置において第３８図のステップ８７６ａ、８７６ｃ、８７６ｅ、８７６ｆに示す照合ルーチンによりステップ８７６ｅで現実にディスクから抽出した第２ソフト特徴情報８８５と一致しなくなるため、入れ替えたディスクの再生は防止される。こうして、各ソフトの海賊版防止識別子８６５および後述するサブ公開鍵の不正変更は防止される。このため、海賊版業者がディスクからソフトをコピーして海賊版を作成する場合、海賊版防止識別子やバーコードのないディスクを作成しようとすることが考えられる。この時、海賊版防止識別子８６５の海賊版防止識別子をオン（”１”）からオフ（”０”）へ設定変更する必要がある。しかし、この設定変更には第３６図のステップ８６６ａに示したマスタ秘密鍵により暗号化した第１暗号を鍵管理センタから発行してもらう必要があるが、海賊版業者に鍵管理センタが発行することは通常防止されるため、海賊版防止識別子８６５が不正変更されることは防止される。

つまり、第１ソフト特徴情報８６３と海賊版防止識別子８６５を一括して暗号化した第１暗号８８６を原盤へ記録することにより、海賊版業者は海賊版防止マークや機能のない海賊版無対策のディスクのフォーマットで、海賊版防止機能が付与されているソフトを不法に作成することが防止されるという効果がある。本発明の一つの対応であるこの手法により、海賊版対策のしてないディスクと、対

策してあるディスクとを混在させながらディスク規格を作り、世代交代しても第２世代の再生装置では全てのディスクに対して海賊版防止を実現するという大きな効果がある。尚、上記具体例では、著作権保護フラグ（識別子）として、ソフトコンテンツが海賊版防止の対象ソフトであるか否かを示す海賊版防止識別子８６５等を用いた例を説明した。これとは別に、ソフトコンテンツがコピー防止の対象ソフトであるか否かを示すコピー防止識別子を用いることにより、本来、コピー防止であるソフトのディスクが、コピー防止識別子を解除されて、ディスクの形態で販売されることを防止できる。

ここで、公開鍵系秘密鍵において、上記マスタ秘密鍵とサブ秘密鍵の必要性及びさらにそれら秘密鍵の具体的な構成、作用について詳述する。

本発明の海賊版防止においては二次記録できるため暗号用秘密鍵をディスク工場に渡す必要はない。しかし、全世界で生産される全てのディスク１枚毎に、暗号化センターに暗号エンコードしてもらい、暗号をネットワークで受けとる方式は通信のトラフィック量が多くなるため現実的でない。かといって、各ソフトメーカーやディスク工場に秘密鍵を渡すことはセキュリティの面で、できないという問題点がある。この問題点を解消する方法が求められている。

本発明ではこれを解消する方法としてマスタ鍵、サブ鍵方式を提供する。本発明では、鍵管理センタ（鍵発行センタ）がマスタ秘密鍵をもち外部に公開しない。一方、ソフト会社はサブ秘密鍵をもつことにより、自分のソフトのセキュリティを自分の責任で確保する。第３２図を用いて、上述したように、ソフト特徴情報と各ソフト会社がもつサブ公開鍵を一括してマスタ秘密鍵で暗号化し、それを第１暗号とする。再生装置では第１暗号をマスタ公開鍵で復号し、その復号されたものからサブ公開鍵が抽出される。そのため、マーキングの位置情報を暗号化し

たものとしての第２暗号を復号するのに必要となるサブ公開鍵は、不正な変更ができない。

従って、特定のソフトは特定の秘密鍵つまり、各ソフトメーカーがもつサブ公開鍵の秘密鍵でしか暗号化されないこととなる。各ソフトメーカーはこのサブ秘密鍵を用いて自由にソフトの鍵の開閉を設定できる。

逆に海賊版業者は、ソフト毎に異なるサブ秘密鍵の情報をそのソフトメーカーから盗まない限り海賊版が製造できないことになる。

ソフトメーカーは、第３２図において、ディスク物理位置情報８６８とディスクＩＤ８６９を合成して、サブ秘密鍵８７６（第３２図に合わせるために、符号を修正しました。以下同様）でステップ８６６ｆで暗号化して公開鍵系暗号８５９を作成し、光ディスク８００にバーコード記録する。この場合、マスタ秘密鍵８６６ａをソフトメーカーに渡さないでソフトメーカーがサブ秘密鍵８７６で海賊版防止ディスクを製造することができる。このため、マスタ秘密鍵のセキュリティが確保できるという効果がある。もしサブ秘密鍵が盗まれて海賊版ディスクが生産されても、その被害はサブ秘密鍵を発行したソフトのみに限定される。ソフトメーカーは新しいサブ秘密鍵とサブ公開鍵を発行すれば、それ以降のソフトの海賊版ディスクの生産は防止される。第３６図、第３７図の全体のシステム図に、データの流れを示す。

第３６図は第３２図と同じ動作であるので詳しい説明は省略する。第３６図においてソフト会社８７１ａではまず各社独自のサブ秘密鍵８７６を設定し、演算することによりサブ公開鍵８６１が求められる。このサブ公開鍵８６１を、記録対象のソフトのソフト特徴情報８６３と合成し鍵発行センター８７２にインターネット等のネットワークで送信する。鍵発行センター８７２ではマスタ秘密鍵８

６６ａで合成信号を暗号化しマスタ公開鍵暗号８５８をソフト会社へ返信し、ソフト会社では、ソフトと合成し合成信号をディスク工場８７３へ送り原盤８６７に記録し、ディスク８００が製造される。第３７図へ進み、ソフト会社８７１ｂではディスク８００にマーキングを行い、マークの位置情報を読みとり、位置情報をサブ公開鍵に対応したサブ秘密鍵８７６により、暗号化しディスク８００ｂにパルスレーザー８１３でバーコード記録する。詳しい記録の動作は説明済みのため省略する。

次に、このようにして、作成された光ディスクを再生する場合の、再生装置における海賊版防止の動作を第３８図を用いて、さらに詳しく具体的に説明する。

まずこの動作は大きく、ソフト照合ステップ８７４とディスク照合ステップ８７５に分けられる。ソフト照合ステップ８７４のステップ８７６ａでは、まず、ディスク８００より第１暗号を再生し、ステップ８７６ｃで再生装置のＲＯＭに入っているマスタ公開鍵を用いて、ステップ８７６ｂで、第１暗号を平文化する。ステップ８７６ｄで第１ソフト特徴情報８６３とサブ公開鍵８６１の平文を入手し、ステップ８７６ｅで、一方向性ハッシュ関数を用いて抽出した第２ソフト特徴情報とを、ステップ８７６ｆで照合する。ステップ８７６ｇで照合が正しくない時は動作を停止し、正しい時は、ステップ８７６ｈでサブ公開鍵を出力させる。海賊版業者がサブ公開鍵やソフト属性を変更した場合、照合が一致せず、不正再生は阻止される。こうして正規のサブ公開鍵が再生装置において得られる。

ディスク照合ステップ８７５のステップ８７６ｋではサブ公開鍵を入力し、ステップ８７６ｍでは第２暗号つまり公開鍵系暗号８５９（第３２図参照）を再生し、ステップ８７６ｎではサブ公開鍵を用いて平文化し、ステップ８７６ｐでマークの位置情報を得る。この場合、マークの位置情報はサブ公開鍵のサブ秘密鍵

８７６（第３２図参照）が漏れない限り改ざんされない。ステップ８７６ｐでレーザによりディスクに形成されたマーキングの現実の位置を読み取り、ステップ８７６ｒで照合する。ステップ８７６ｓでＮｏならステップ８７６ｔで停止し、“海賊版ディスクです。”という表示を出す。Ｙｅｓならステップ８７６ｕで再生を続ける。

以上のような再生装置の構成により、不正に複製したディスクについては、ソフトメーカー保有のサブ秘密鍵８７６が盗まれない限り、また無反射部のマークを超サブミクロン例えば０．１３μｍの精度でレーザートリミングさせかつ２枚のディスクをミクロンオーダーで正確に貼り合わせない限り、再生装置において再生動作が行われない。従って、事実上、海賊版を作ることはできない。これにより海賊版が防止されるという効果がある。

（ｃ）公開鍵系と秘密鍵系の暗号関数を併用する例のより詳しい説明：

本実施例の暗号化における第１の特徴としては、１枚毎の光ディスクにおけるマーキングの位置情報等を暗号化する際に、公開鍵系暗号関数と秘密鍵系暗号関数の２つの関数を用いている点である。

ここでは本発明による公開鍵系暗号を用いた海賊版防止方式を現実に実用化する場合の課題と実現方法を述べる。尚、公開鍵系暗号とは、上述した位置情報を公開鍵系暗号関数（例えば、ＲＳＡ関数）を用いて、暗号化したものをいう。

機密性保持の面からは、全ての再生装置に公開鍵系暗号復合器を設けて本発明の海賊版防止の公開鍵系暗号を復号するのが望ましい。しかし、５１２ｂｉｔの公開鍵暗号をＣＰＵで処理する時間は、３２ｂｉｔ５０ＭＨｚのＣＰＵを用いて０．３秒を要する。一方、現在の民生機器のＤＶＤプレーヤ制御用ＩＣは８ｂｉｔの１ｃｈｉｐマイコンが主流である。このＣＰＵでは公開鍵を処理するのに数

分以上かかる。これは数分待たないとＤＶＤの画像が出てこないことになり、製品には導入できないといった課題がある。

このように現時点では、公開鍵系暗号は、民生用製品のＣＰＵでは処理できないため、当分の間、民生用の再生機器は処理量の少ない秘密鍵系暗号用復号器を搭載せざるを得ない。秘密鍵系暗号は、暗号デコーダの情報から暗号化秘密鍵を容易に逆解読することができるため、その時点で秘密鍵系暗号は海賊版防止効果がなくなる。従って将来、逆解読が困難な公開鍵系暗号に移行させることが不可避といえる。

秘密鍵系暗号と公開鍵系暗号には、全く互換性がない。このため、将来、単純に秘密鍵系暗号を公開鍵系暗号に切り換えると、秘密鍵系暗号デコーダをもつ第１世代のプレーヤで、公開鍵系暗号をもつ第２世代の光ディスクを復号・再生できなくなる。また第１世代の秘密鍵系暗号をもつ光ディスクを将来のプレーヤで再生することもできなくなる。もし、この再生を可能に設定すると、海賊版業者は秘密鍵系暗号の秘密鍵を逆解読し、これを用いて秘密鍵暗号を作成し、海賊版ディスクを作成するので、海賊版ディスクが大量に販売されることになる。秘密鍵系で暗号化されたディスクを将来のプレーヤでも再生可能とした場合、公開鍵系暗号を使っても海賊版は防止できない。

このことから、将来、秘密鍵系から公開鍵系へ再生装置の暗号デコーダが移行しても、新しい公開鍵系暗号デコータをもつ再生装置で初期の光ディスクを正常に再生し、かつ海賊版ディスクの不法再生を防止する互換性維持の工夫が必要となる。

この互換性の要求を満たす本発明の方法を開示する。第３９図に示すように本発明の光ディスクでは秘密鍵系暗号記録部８７９と公開鍵系暗号記録部８８０の

双方をもつ。製造方法は第２９図を用いて後述する。まず第３９図のこの光ディスクを再生する時、第１世代の秘密鍵系暗号デコーダ８８１をもつ再生装置では、正規ディスクの秘密鍵系暗号記録部８７９から秘密鍵系暗号デコーダ８８１によりディスク固有の第１物理特徴情報（位置情報が暗号化されたものに対応）を平文化する。又、ディスクの第２物理特徴情報（測定された位置情報に対応）を測定し、双方の物理情報を照合する。

正規ディスクの場合は、ステップ８７８ａに示すように双方の物理特徴情報が一致するので通常に再生される。

海賊版ディスクの場合は、ステップ８７８ｃに示すように照合結果が一致しないので、不正再生は防止される。秘密鍵系暗号が破られるまでは防止されるが、上述のように将来、秘密鍵系暗号が破られた後は海賊版業者は秘密鍵系暗号を不正生成することにより不正ディスクを大量に作成する。

従って、ステップ８７８ｄに示すように第１世代の再生装置の秘密鍵系デコーダ８８１では秘密鍵系暗号しかチェックしないので照合結果が一致し、海賊版ディスクが不正に再生される。しかし、将来のこの時点においては第２世代の公開鍵系暗号デコーダ８８２をもつ再生装置が大勢を占めているため、第１世代の再生装置における海賊版ディスクの不正再生の影響は小さい。

この第２世代の再生装置では、本発明の正規ディスクは公開鍵系暗号をもつためステップ８７８ｂに示すように正常に再生される。一方、海賊版ディスクを再生した場合、秘密鍵系暗号の逆解読のいかんにもかかわらず、ステップ８７８ｅに示すように再生装置は公開鍵系暗号のみをチェックするため、ステップ８７８ｅに示すように、公開鍵系暗号の海賊版防止機能が働き、第２世代の再生装置では海賊版がほぼ完璧に防止される。

本発明の場合、全てのディスクに秘密鍵暗号８７９に加えて公開鍵暗号８８０を第１世代の再生装置の出荷段階から予め搭載してある。従って、まず第１段階では第１世代の再生装置の８ｂｉｔマイコンで暗号の処理ができるため、秘密鍵系暗号レベルの海賊版防止ができる。次に第２段階つまり将来、秘密鍵系暗号が破られた時点においては、主流となっている第２世代の公開鍵系暗号デコーダにより完全な海賊版防止ができる。このため、世代交代が起こっても初代のメディアとの互換性を完全に保ちながら第２世代の再生装置により中断することなく、海賊版防止がほぼ完璧に実現するという世代交代時の互換性を確保する効果がある。

なお、上記説明では低反射部マーキング方式、つまり反射層レベルの海賊版防止方式に適用した場合の例を説明したが、第１３図のような原盤の物理特徴情報を用いる原盤レベルの海賊版防止方式に適用しても同様の世代交代時の互換性を確保する効果が得られる。

以上説明した例では、暗号化を行なう場合、同一の暗号化対象を、公開鍵系暗号関数と秘密鍵系暗号関数を個別に利用して、それぞれ暗号化し、この双方をディスク上に記録することを特徴としている。

従って、現行の８ビットマイコンによる秘密鍵系暗号関数により暗号化された暗号を復号する復号器を持ったプレーヤーから、将来の３２ビットマイコンによる公開鍵系暗号関数により暗号化された暗号を復号する復号器を持ったプレーヤーに移行しても、本例による光ディスクであれば、何れのタイプのプレーヤーに対しても、有効に使用できるという効果がある。

（Ｂ）その他の工夫について説明する。

（ａ）次に、別の具体例として、公開鍵系と秘密鍵系の併用タイプであり、そ

の暗号化対象となるものが、ソフト特徴情報、ＩＤ番号、マーキングの位置情報の場合について説明する（第２９図参照）。ここで、ＩＤ番号とは、ディスク毎に与えられた、各ディスクを識別するための番号である。後述するディスクＩＤ（ディスクＩＤ番号とも呼ぶ）も、このＩＤ番号と同じ意味である。本例と上記具体例（第３２図、第３６図、第３７図参照）との主なる相違点は、（１）上記具体例では、ソフト特徴情報は、ディスクの原盤に第１暗号として書き込まれ、一方、マーキングの位置情報は、成型されたディスクに第２暗号として書き込まれるのに対して、本例では、ソフト特徴情報、ＩＤ番号、マーキングの位置情報の全てが合成されて暗号化され、既に成型されたディスクに書き込まれるという点である。又、（２）上記具体例では、マスタ秘密鍵とサブ秘密鍵を利用して、２段階の暗号化を行うのに対して、本例では、サブ秘密鍵に対応する鍵は使用せず、言うならばマスタ秘密鍵による暗号化を行う点である。

即ち、第２９図に示す様に、秘密鍵系秘密鍵８３４により、上述の合成された信号を秘密鍵系暗号化部８３２においてエンコードする。又、公開鍵系秘密鍵８３３により、上述の合成された信号を公開鍵系暗号化部８３１においてエンコードする。このように、公開鍵系と秘密鍵系の暗号を併用する。これにより、現在の再生装置はマイコンの処理速度が遅いため、秘密鍵系暗号しか復号できない問題点が、解決できる。将来の再生装置は３２ビット等の処理速度が速いマイコンを用いてセキュリティが強い公開鍵系のみを復号し、海賊版チェックを行うので、海賊版は、ほぼ完全に防止できる。秘密鍵系が将来被られても、その時点においては公開鍵系プレーヤが大勢を占めているので、海賊版は実質的に防止できる。秘密鍵系と公開鍵系暗号を同時に媒体に記録しておくことによりプレーヤの世代交代が起こっても旧世代のプレーヤで再生できるとともに実質的に海賊版が防止

できるという効果がある。

（b）次に、同図を用いて、更にバーコードの変調記録方式について詳細に述べる。

第２９図において、バーコード記録装置（PWM記録装置）８４５は、ディスクに暗号化された情報を書き込むためのものである。

まず、反射層８０２、又は第２反射層８２５に設けられた無反射部８１５の位置情報を光マーク位置検出手段６００で検出する。この検出方法は第１５図等を用いて説明したので省略する。光マーク位置情報と、ＩＤ発生部５４６によるＩＤ番号と、ソフト特徴情報とを合成手段８３０により合成する。ソフト特徴情報はソフトコンテンツの一部をＳＨＡ等の一方向ハッシュ関数で特徴抽出し１２８ビットや１６０ビットのハッシュ値を求めることにより得る。ＩＤ番号発生部５４６は、第１４図を用いて説明したので省略する。この物理特徴情報の合成信号を暗号化部８３０において公開鍵系秘密鍵８３３を用いてＲＳＡ等の公開鍵系暗号化部８３１においてエンコードする。

上記の公開鍵系の暗号と、秘密鍵系の暗号を合成部８３５で合成し、記録回路８３６のエラー訂正符号化部８３７の中で、リードソロモン符号化部８３８とインターリーブ部８３９によるインターリーブ／リードソロモンのエラー訂正を行う。この場合のインターリーブ長はディスク上のバーストエラーとしてＣＤ並みつまり、２．３８ｍｍ以上の長さの傷によるバーストエラーに対して、エラー訂正できるように設定することにより、民生用途の最悪条件で発生するディスク上の傷に対して、本発明のバーコード記録データのエラーが訂正されるという効果がある。

更に、同図を用いて、パルス巾変調方式の原理を述べる。また、この方式はマ

スタ秘密鍵による第１暗号とサブ秘密鍵による第２暗号を使わなくてもよい。この方式では、ソフト特徴情報と位置情報とＩＤ番号を合成して暗号化している。年間数十億枚ＲＯＭディスクは生産されている。このためディスクのマークが偶然非常に複製しやすい位置パターンのディスクが製造される可能性がある。この複製しやすい位置情報のマークとこの位置情報の正規の暗号の組み合せで、海賊版が製造されてしまう。第２９図においては、位置情報がソフト特徴情報とともに暗号化もしくは署名されている。従って、この位置情報は、このソフト特徴情報と切り離せない。つまり、複製容易なマークが製造できても、それに対応するソフトコンテンツの海賊版ディスクしか製造できず、被害が、大巾に限定されるという効果がある。なお、この暗号は原盤に記録しても良い。

エラー訂正符号化された信号はパルス間隔変調部８４０により、ＰＷＭ信号に変調される。レーザーにより直線を描く場合、線巾を正確に制御してバーコードを作成することは難しい。従って、第３０図に示すように、本発明ではパルス間隔を１Ｔ，２Ｔ，３Ｔ，４Ｔの４値に更け分けマーク８４３ｂ，８４３ｃ，８４３ｄ，８４３ｅを各々例えば００，０１，１０，１１と符号化することにより、２ｂｉｔのデータを１本のバーコードで伝送することができる。第３０図の線巾と記録速度の関係表８４２に示すように、線巾＝１０μｍの時、ＲＯＭディスク８００のリードインエリアにＰＩＭバーコードを記録した場合、１周で５．６Ｋｂｉｔの情報がディスクの完成品に追記記録できることがわかる。

第３１図の信号（１）は無反射部の検出信号を示す。

まず、信号群は、間隔Ｔの３本のパルス８５７ａ，８５７ｂ，８５７ｃからなる開始位置を示す同期信号領域８５８がある。次に基準時間Ｔを測定する基準時間Ｔを測定する基準時間領域で４Ｔのブランクがある。線幅１０μｍの場合Ｔ＝

２０μｍである。そして２次記録データが入っている第１記録領域８６０が約１Ｋｂｉｔである。そして１００μｍ以上のブランク８６１ａを空けて、３回目の記録、３次記記録データの第２記録領域８６２ａが記録される。具体的には、販売店で、スクランブル解除用のパスワード等が記録される。

（ｃ）このＨＭＳＴ方式で二次、三次記録できるバーコードの利用方法について述べる。

第３５図に示すようにソフトメーカーでは、工程（２）ではディスク１枚ごとに異なるＩＤ番号やユーザーとの秘密通信用のプライベートキーを記録したディスク８４４ｂを作成しても良い。このディスク８４４ｃ，８４４ｄは何もしなくとも再生できる。

又、後述する第２１図において示したように、磁気記録再生回路のＭＦＭ変復調部磁気ヘッドをＰＷＭ（ＰＩＭ）変復調部レーザーに置き換えることにより、本発明のＨＭＳＴ方式の記録再生回路が得られる。

（ｄ）ここで、第３５図において、ディスク作成の別の具体例を示す。即ち、別の応用として、第３５図に示す工程（３）では、スクランブルしたＭＰＥＧ映像信号等の情報をディスク８４４ｅに記録する。ここで、ＭＰＥＧスクランブルの動作説明を簡単に行う。ＭＰＥＧの画像圧縮信号はＡＣ成分の可変長符号部と固定長符号部に分けられ、各々に乱数加算部があり、スクランブル化される。本発明では、スクランブル解除信号を一方向関数の暗号エンコーダーで暗号化する。また、画像圧縮制御部の圧縮プログラムの一部を暗号エンコーダーにより圧縮している。このため、複製業者が暗号エンコーダーを不正なものに入れ替えることが困難となる。従って、正規のディスクのみがサブ公開鍵で復号される。

次に、再び、第３５図に戻り、上述した工程（３）で作成されたディスク８４

４ｅに対しての、次の工程（４）以降での処理の内容を説明する。

即ち、第３５図において、ソフト会社では同図に示す工程（４）においてディスクＩＤ番号とスクランブル解除情報を復号するためのサブ公開鍵をマスタ秘密鍵で暗号化した暗号をバーコードで二次記録したディスク８４４ｆを作成する。このディスク８４４ｆは、スクランブルされているので、このディスク単独では再生はできない。ここで、ディスクＩＤ番号は、上述したＩＤ番号と同じ意味である。工程（５）では、販売店が客からディスクの代金を受け取った後にサブ公開鍵に対応しているサブ秘密鍵でディスクＩＤ番号を用いてパスワードを作成し、ディスクに三次記録する。このあとは、ディスク８４４ｇにはパスワードが記録されているため、再生装置でディスクスクランブルされ再生可能となる。コンピュータプログラムの場合はインストール可能となる。この方式を用いると、代金の支払われていないディスクが万引きされても映像のスクランブルや暗号化が解除されないため画像やソフトが再生されない。このため、万引きが無意味になり、防止されるという効果がある。

（ｅ）ここで、一旦、第３５図を利用した説明を終えて、第２１図を参照しながら同図に示す記録回路のついた再生装置として、光再生装置に磁気記録再生回路を組み合わせた記録再生回路における磁気記録再生回路を中心に構成及び動作を説明する。尚、第２１図では、光再生装置と合体した磁気記録再生回路を用いて説明しているが、通常の光再生装置とフロッピイドライブの組み合せでもよい。

同図では磁気再生回路の中の復調器としてＭＦＭ復調器３０ｄとは別の方式の第２復調器６ｂ２をもち、切換部６６１で切り換えられる。これは対応する変調器は工場しかもたないため、再生はできるが完全な記録はできない。従って、工場で特殊変調された領域を記録した場合、特殊変調信号は記録されない。ドライ

プ側ではＣＰＵ６６５により、この領域で特殊変調信号を再生しない限り、記録できないように制御している。従って、論理的な、Ｗｒｉｔｅ　Ｏｎｃｅ領域といえ、１回だけ記録できる。従って再生装置のＲＯＭ６９９に記録されたドライブＩＤ６９９ａ等のマシンＩＤを、光ディスクの磁気記録部もしくはフロッピイディスクのＷｒｉｔｅ　Ｏｎｃｅ領域に記録すると、ユーザーのドライブでは改ざんすることができなくなり、許可された台数以上の不正インストールを防止することができる。ここで、ドライブＩＤとは、再生装置毎に与えられた、各再生装置を識別するための番号である。また、このマシンＩＤはパソコンのＩＤでもよい。ネットワークのインターフェース部１４により、ネットワーク６６４に、接続された第２パソコン６６３の中のＨＤＤ等をみて、同じドライブＩＤやマシンＩＤ番号のプログラムが起動や動作をしないように監視させる。こうして、不正コピーされたソフトの動作を防止する。

また、本発明のレーザでマーキングする記録方式を用いると磁気方式のようにディーラーでディーラーコードを記録したり等の二次記録ができるが、本発明の特徴的な部分ではないので、詳しい説明はここでは省略する。

レンタルビデオ店では恒久的にパスワードを記録すると、万引きされた場合、使用されてしまう。この場合は工程（６）に示すように、レンタル店でスクランブルされているディスク８４４ｊを客に渡す。ステップ８５１ｇでスクランブル解除のためのパスワードは、ディスクＩＤもしくは後述するドライブＩＤをサブ秘密鍵を用いて算出する。ステップ８５１ｊでプリンタでレシートに印刷して、客に手渡す。ステップ８５１ｕに示すように電話等で客に通知しても良い。

客は自宅の再生装置においてステップ８５１ｒのスクランブル解除処理を行う。まずステップ８５１ｓで暗号よりスクランブル識別子とソフト特徴情報とサブ公

開鍵で復号化する。復号されたソフト特徴情報と実際にソフトコンテンツから一方向ハッシュ関数で抽出したソフト特徴情報を照合し、一致しているか検証する。検証できない時は、不正とみなし、ストップする。ステップ８５１ｘでスクランブル識別子がＯＦＦの場合は、ステップ８５１ｐで再生を許可する。スクランブル識別子がＯＮの場合はステップ８５１ｋでユーザがパスワードをテンキーで入力し、パスードはサブ公開鍵で演算する。ステップ８５１ｔでさらにディスクＩＤもしくは／かつドライブＩＤを用いた演算を行ないパスワード演算結果がディスクＩＤもしくはドライブＩＤにする場合のみ、ステップ８５１ｐで、スクランブルもしくは暗号化を解除し、再生もしくは動作を所定の日数だけ許可する。ディスクの一部のソフトのパスワードのみを与えてレンタルした場合に、他のソフトをみたくなった時は、鍵発行センターへ電話し電話で、そのソフトのパスワードをステップ８５１ｕで通知してもらい、ステップ８５１ｋで入力することにより、ディスクの他のソフトを再生することができる。

第３５図の工程（５）（６）のセルビデオ販売店、レンタルビデオ店における動作を第３４図を用いてより具体的に説明する。セルビデオ販売店ではソフトメーカーからスクランブルもしくは暗号化がかかったディスク８４４ｆを受けとり、ユーザーからの入金を確認するとバーコード記録再生装置８４５よりディスク８４４ｆのディスクＩＤ番号、サブ公開鍵のデータをＰＯＳ端末８４６経由でパスワード発行センター８５２に送信する。小規模な店舗システムの場合パスワード発行センター、つまりサブ公開鍵のサブ秘密鍵を含むシステムはＰＯＳ端末の中にあっても良い。パスワード発行センターはステップ８５１ｑでディスクＩＤ番号と時間情報を入力し、ステップ８５１ｓで演算を行い、ステップ８５１ｔで、サブ秘密鍵を用いて暗号化し、ステップ８５１ｇでパスワードを発行しネットワ

ーク８４８とＰＯＳ端末８４６を介してバーコード記録装置８４５にパスワードを送り、記録されたディスク８４４ｇが客に渡される。このディスク８４４ｇは、そのまま再生できる。

次にレンタル店における動作を詳しく述べる。まずスクランブルの解除されていないＲＯＭディスク８４４ｆを店頭に陳列する。客が特定のＲＯＭディスク８４４ｆを指定した場合、うずまき型にスキャンする回転型の光学ヘッド８５３を内蔵した円形バーコードリーダ８５０を手にもち、透明ケース入りのディスク８００の中心におしつけることにより、ディスク８４４ｆの無反射部８１５による反射層のバーコードを読み取り、ディスクＩＤ番号を読み取る。商品コードは無反射部８１５の本発明のバーコードから読みとってもよいし、原盤のピット記録領域外の内周部に予め記録されプレスされた既存の記録方式による円形バーコードから読みとっても良い。これらの情報はＰＯＳ端末８４６により処理され、レンタル料金が決済されるとともに、前述のようにディスクＩＤ番号に対応したパスワードがステップ８５１ｇにおいて発行される。レンタル用途の場合、視聴可能な日数を制限するためステップ８５１ｒで用いたように日付情報を加えて、ディスクＩＤ番号を暗号化しパスワードを作成する。このパスワードの場合、特定の日付しか作動しないため、レンタルの場合例えば３日間の貸し出し期間をパスワードの中に設定できるという効果がある。

さて、こうして発行されたスクランブル解除のためのパスワードはステップ８５１ｉにおいて、貸出日、返却日、レンタルのタイトル料金とともにレシート８４９に印刷され客にディスクとともに渡される。客はディスク８４４ｊとレシート８４９を持ち帰り、ステップ８５１ｋでパスワードを第２５図の情報処理装置６７６のテンキー等の入力部８５４に入力することによりパスワードはディスク

ＩＤ番号と演算されてマスタ暗号デコーダ５３４に入力され、公開鍵を用いて平文化される。この平文が所定の条件を満たすか平文データ照合部７１５で照合され、正しいパスワードである場合のみサブ暗号デコーダ７１８でプログラムのデータをデスクランブルし、映像出力させる。

この場合、パスワードに時間情報が含まれている場合、時計部８５５の日付データと照合し、一致した日付の期間、デスクランブルをする。なお、この入力したパスワードは対応するＩＤ番号とともにメモリ７５５の不揮発メモリ７５５ａにストアされ、ユーザーは一度パスワードを入力すると２度と入力することなしにデスクランブルされる。こうして流通において電子的にディスクの鍵の開閉ができるという効果がある。

これまでの実施例では、主にディスクにディスクＩＤ番号を付与したディスクＩＤ方式を用いて、説明した。しかしディスクにディスクＩＤがついていない場合は、ドライブのドライブＩＤを利用する必要がある。ここでは、ドライブＩＤを単独で用いた場合およびドライブＩＤとディスクＩＤの双方を用いた場合のスクランブル解除のパスワードの作成と照合の動作につい具体的に説明する。

第３５図においてソフトのスクランブル解除用にドライブＩＤに関連するパスワードを用いる場合は、まず、再生装置のＲＯＭ内のドライブＩＤ６９９ａを電話もしくはパソコン通信により、第３４図の信号部８５１ｚからパスワード発行センターへ送信する。パスワード発行センターでは、ステップ８５１ｑでこのドライブＩＤとソフトのＩＤを用いて、ステップ８５１ｓで演算しステップ８５１ｔでサブ秘密鍵により暗号化し、ステップ８５１ｇでパスワードを作成する。ステップ８５１ｕで、パスワードを、電話もしくは、パソコン通信を用いてユーザーのパソコンを含む再生装置の通信部８５ｚへ送信する。ユーザーはステップ８

５１ｋにおいてパスワードを入力し、ステップ８５１ｍでサブ公開鍵で復号演算する。ステップ８５１ｔで、ドライブＩＤと演算結果を照合し、一致しない時は停止し、一致する時はステップ８５１ｐで再生もしくは動作を実行する。

ここでドライブＩＤの方式とディスクＩＤ方式の得失について述べる。ディスクＩＤを用いた場合は、パスワードはそのディスク１枚にのみ有効である。従って、全てのドライブで動作するため、映画ソフト等に適している。しかし、パソコンのビジネスソフトの場合は、どんなドライブでもインストールできると、１枚のディスクから複数のパソコンに不正インストールされてしまう。

ドライブＩＤ方式が、１台のドライブでしか動作しない点が映画ソフトでは欠点になる。しかしパソコンソフトの場合は利点となる。１回しかインストールする必要のないビジネスソフトの場合、ドライブＩＤ方式のパスワードプロテクト解除方式により正規の１台のドライブ以外のドライブを用いてパソコンに不正インストールできないという効果がある。

しかし、ドライブＩＤはマシンのＥＰＲＯＭにＩＤを書き込むだけであり、容易に改ざんされる。このため、同じドライブＩＤのドライブが販売されると、大量に不正インストールされるおそれがある。一方、本発明のディスクＩＤの改ざんが困難であることを述べた。第３４図のステップ８５１ｑにおいてディスクＩＤとドライブＩＤとドライブの双方のパスワードを作成し、ステップ８５１ｔで両方のＩＤをチェックするように変更することにより、ディスクＩＤの方は改ざんされない。このため、同じドライブＩＤのドライブが大量に出回っても、ディスクＩＤが１枚しか存在しないことにより、大量の不正インストールが抑制されるという効果がある。

また上述のように、ドライブＩＤ方式とディスクＩＤ方式は各々利点と欠点を

もち、用途により利点が異なる。１回インストールするだけのコンピュータソフト用には主にドライブＩＤ、何回も再生する映画、音楽ソフトにはディスクＩＤが使われると思われる。従って、再生装置は両方に対応する必要がある。図４２のフローチャートを用いてドライブＩＤとディスクＩＤの双方に対応する動作を説明する。インストールが開始されると、まず、ステップ９０１ａでスクランブル識別子がＯＮかどうかをチェックする。識別子がＯＦＦの場合にソフトがスクランブルされている場合は不正であるので停止する。ＯＮの場合にソフトがスクランブルされていない時も停止する。既に述べたように、このスクランブル識別子は改ざんできないため不正を防ぐことができる。ステップ９０１ｃでパソコンをネットワークによりパスワード発行センターに接続する。ステップ９０１ｄでユーザーＩＤを入力し、ステップ９０１ｅで再生装置のドライブＩＤがある時はドライブＩＤをパスワード発行センターへ送信する。パスワード発行センターでは入金を確認した後、ドライブＩＤとソフトＩＤから暗号のサブ秘密鍵を用いて、暗号化と演算を行いパスワード生成し、ユーザーのパソコンではパスワードをサブ公開鍵で演算、複号し、パソコンのマシンＩＤもしくは、ドライブのドライブＩＤと照合する。照合が一致しない場合は停止し、照合が一致した場合はステップ９０１ｎでインストールプログラムを動作させる。この場合、具体的にはステップ９０１ｋでパスワードをドライブＩＤ番号と演算する時、プログラムの暗号解除キーを出力して暗号もしくはスクランブルを解除してもよい。

さてステップ９０１ｅに戻り、ドライブＩＤがない時はステップ９０１ｈでディスクにディスクＩＤが記録されているかをチェックし、ディスクＩＤがない場合は停止する。ディスクＩＤがある時は、ステップ９０１ｃでディスクＩＤとソフトＩＤをパスワード発行センターへ送信する。パスワード発行センターではク

レジット会社と交信しクレジットによるオンライン入金決済確認後ステップ９０１ｊでディスクＩＤとソフトＩＤにより、サブ秘密鍵を用いてパスワードを作成する。ユーザーのパソコンではステップ９０１ｍでこのパスワードをサブ公開鍵で復号し、照合ＯＫならプログラムインストールもしくはソフトの再生を実行する。

このように、ドライブＩＤ、ディスクＩＤのどちらにも対応できるので、様々なＩＤをもつソフトに対応して不正インストールを防止しながら正規インストールできるという効果がある。

このようにして、ディスクの物理ＩＤを一方向性の暗号エンコーダにより暗号化することにより複製防止の安全度を高めることができる。

以上のように、本実施例によれば、２枚のディスクを張り合わせた光ディスクの反射層上に無反射部を作成し、少なくともその位置情報を暗号化して、同じ光ディスク上に書き込むことにより、従来に比べてより一層複製が困難となる。これにより、不正な複製を行う、いわゆる海賊版の作成を事実上不可能にすることができる。

以上述べたところから明らかなように本発明は、複製防止能力を従来に比べてより一層向上させることが出来るという長所を有する。

なお、本実施例によれば、暗号化の工夫において、第３２図等を用いて説明した様に、フォーマットの原盤物理特徴情報８７６を公開鍵データやソフト特徴情報と合成して暗号化することにより原盤にも海賊版防止チェックをかけられるのでよりセキュリティが高くなる。

又、第２６図ではオンラインショッピング会社のネットワークセキュリティを向上させる方法を開示したが、秘密通信用のプライベートキーをオンラインショ

ッピング会社が全ディスクに予め二次記録しユーザーに配布することによりプライベートキーを封書でユーザーに送る必要がなくなり、ユーザも長い桁数のプライベートキーをキー入力する手間が省ける。また、ユーザ入力でなくなるため、プライベートキーとして、１００桁以上の長い数値を用いることができるためネットワークセキュリティが大巾に向上する。

又、本発明のマーキングの位置情報は、上記実施例では、同じディスク上に書き込む場合について説明したが、これに限らず例えば、他の媒体としての他のフロッピーディスクに書き込むようにしてもよい。

又、上記実施例では、ディジタル署名の技術又はディジタル署名的な技術又は暗号化技術に、楕円関数やＲＳＡ関数を応用した場合について説明したが、それに限らず、例えば、ＤＥＳの秘密鍵系暗号関数等、その他の暗号化に関するいかなる技術を利用してもよいことは言うまでもない。

又、上記実施例では、位置情報を暗号化又はディジタル署名していたが、そのようなことはせずに、位置情報そのものをディスクに書き込んでもよい。その様な場合でも、マーキングとその位置情報をコピーして海賊版を作ることに対しては有効である。

又、本発明の、レーザにより消滅しない材料からなる２つの部材により反射膜が直接又は間接的に挟まれた構造を備えたディスクであって、その反射膜にレーザーによりマーキングが施されていることを特徴とする光ディスクは、上記実施例では、海賊版防止技術に利用した場合について説明したが、これに限らずその他の技術に応用してももちろんよい。又、本発明のこの光ディスクは、上記実施例では、接着層を間に設けて２枚の基板を張り合わせたディスクについて説明したが、これに限らず接着層は無くてもよいし、あるいは、保護層の様な他の部材

が存在してもよく、要するに、レーザにより消滅しない材料からなる２つの部材により反射膜が直接又は間接的に挟まれた構造であればよい。更に又、本発明のこの光ディスクは、上記実施例では、張り合わせるものととして、基板を用いた場合について説明したが、これに限らず例えば保護層等他の部材であってもよく、要するにレーザにより消滅しない材料からなる部材であればよい。

又、上記実施例では、世代の異なる複数の暗号の組み合わせ例として、秘密鍵系の暗号と公開鍵系の暗号の２つの暗号を組み合わせた場合を代表例として説明した。しかしながらこれに限らず、世代の異なる別の組み合わせとして、例えば、２５６ビットの秘密鍵を持つ公開鍵系暗号のように安全性は低いが、遅いＣＰＵで処理出来る暗号と、１０２４ビットの秘密鍵を持つ公開鍵系暗号のように安全性は高いが、高速のＣＰＵでないと処理出来ない暗号との組み合わせのように、安全性のレベルの異なる公開鍵系暗号の組み合わせでも、同様の世代交代時の互換性保持効果が得られる。また、秘密鍵系と低安全度の公開鍵系暗号と高安全度の公開鍵系暗号の３つの世代の異なる暗号の組み合わせでもよい。

産業上の利用可能性

以上説明したように、本発明は、例えば、データの書き込まれたディスクの反射膜にレーザーによりマーキングが施されており、少なくともそのマーキングの位置情報又はその位置情報に関する情報が、暗号化され、あるいはディジタル署名された形で、前記ディスクに書き込まれている光ディスクであり、これによって、複製防止能力を従来に比べてより一層向上させることが出来た。

請 求 の 範 囲

1． ディスクに形成された反射膜にマーキングを施すマーキング生成手段と、

前記マーキングの位置を検出するマーキング位置検出手段と、

前記検出された位置をマーキングの位置情報として出力する位置情報出力手段と、

を備えたことを特徴するマーキング生成装置。

2． 少なくとも前記出力された位置情報又はその位置情報に関する情報を前記ディスクに、又は別の媒体に書き込むための位置情報書き込み手段を備えたことを特徴する請求項1記載のマーキング生成装置。

3． 前記位置情報書き込み手段は、少なくとも前記出力された位置情報又はその位置情報に関する情報を暗号化する暗号化手段を有し、その暗号化された内容を前記ディスクに書き込むことを特徴する請求項2記載のマーキング生成装置。

4． 前記暗号化手段は、前記暗号化する場合に、公開鍵系暗号関数の秘密鍵又は、秘密鍵系暗号関数の秘密鍵を用いることを特徴する請求項3記載のマーキング生成装置。

5． 前記暗号化手段は、

ディスクに書き込まれるソフト内容の特徴に関するソフト特徴情報と公開鍵系暗号関数のサブ公開鍵とを、前記公開鍵系暗号関数のマスタ秘密鍵により暗号化する第1暗号化手段と、

前記位置情報又はその位置情報に関する情報を前記サブ公開鍵に対応するサブ秘密鍵により暗号化する第2暗号化手段とを有し、

前記少なくとも前記出力された位置情報又はその位置情報に関する情報を書き込むとは、

前記第１暗号手段により暗号化された内容と、前記第２暗号化手段により暗号化された内容とを前記ディスクに書き込むことであることを特徴とする請求項３記載のマーキング生成装置。

６．　前記位置情報書き込み手段は、少なくとも前記出力された位置情報又はその位置情報に関する情報についてディジタル署名を行うディジタル署名手段を有し、

前記少なくとも出力された位置情報又はその位置情報に関する情報を書き込むとは、前記ディジタル署名を行った結果に関する情報を前記ディスクに書き込むことであることを特徴する請求項２記載のマーキング生成装置。

７．　前記ディジタル署名手段は、前記ディジタル署名する場合に、公開鍵系暗号関数の秘密鍵を用いることを特徴する請求項６記載のマーキング生成装置。

８．　前記ディジタル署名手段は、

ディスクに書き込まれるソフト内容の特徴に関するソフト特徴情報と公開鍵系暗号関数のサブ公開鍵とについて、前記公開鍵系暗号関数のマスタ秘密鍵によりディジタル署名する第１ディジタル署名手段と、

前記位置情報又はその位置情報に関する情報について、前記サブ公開鍵に対応するサブ秘密鍵によりディジタル署名する第２ディジタル署名手段とを有し、

前記少なくとも前記出力された位置情報又はその位置情報に関する情報を書き込むとは、

前記第１ディジタル署名手段によるディジタル署名を行った結果に関する情報と、前記第２ディジタル署名手段によるディジタル署名を行った結果に関する情報とを前記ディスクに書き込むことであることを特徴する請求項６記載のマーキ

ング生成装置。

９．　前記位置情報書き込み手段は、同一の対象である位置情報に関して、複数種類の暗号化あるいはディジタル署名技術を用いて処理した情報を並存させるように、書き込みすることを特徴とする請求項２記載のマーキング生成装置。

１０．　前記公開鍵系暗号関数は、ＲＳＡ関数又は楕円関数であることを特徴する請求項４、５、７、又は８に記載のマーキング生成装置。

１１．　前記ディスクは、２枚のディスクを張り合わせることにより作成されていることを特徴する請求項１～１０の何れか一つに記載のマーキング生成装置。

１２．　ディスクの成形を行うステップと、

前記成形されたディスクに反射膜を形成するステップと、

前記反射膜が形成されたディスクを少なくとも１つ含む２枚のディスクを張り合わせるステップと、

その張り合わされたディスクの前記反射層に対して、レーザーによりマーキングの形成を行なうステップと、

を備えたことを特徴する光ディスクのレーザーマーキング形成方法。

１３．　ディスクに形成された反射膜にマーキングを施し、前記マーキングの位置を検出し、少なくとも前記検出された位置がマーキングの位置情報として出力された、そのマーキングの位置情報又はその位置情報に関する情報を読み取る位置情報読み取り手段と、

前記マーキングの現実の位置に関する情報を読み取るマーキング読み取り手段と、

前記位置情報読み取り手段による読み取り結果と、前記マーキング読み取り手段による読み取り結果とを利用して、それらを比較判定する比較判定手段と、

前記比較判定手段の比較判定結果に基づいて、前記光ディスクの記録データを再生する再生手段と、

を備えたことを特徴する再生装置。

１４．　少なくとも前記出力された位置情報又はその位置情報に関する情報は、位置情報書き込み手段により前記ディスクに書き込まれていることを特徴する請求項１３記載の再生装置。

１５．　前記位置情報書き込み手段は、少なくとも前記出力された位置情報又はその位置情報に関する情報を暗号化する暗号化手段を有し、

前記位置情報読み取り手段は、前記暗号化手段に対応する復号化手段を有し、前記位置情報読み取り手段は、前記暗号化された位置情報又はその位置情報に関する情報を前記復号化手段により復号化することを特徴する請求項１４記載の再生装置。

１６．　前記暗号化手段は、前記暗号化する場合に、公開鍵系暗号関数の秘密鍵を用い、

前記復号化手段は、前記秘密鍵に対応する公開鍵を用いて、前記復号化を行うことを特徴する請求項１５記載の再生装置。

１７．　前記暗号化手段は、

ディスクに書き込まれるソフト内容の特徴に関するソフト特徴情報と公開鍵系暗号関数のサブ公開鍵とを、前記公開鍵系暗号関数のマスタ秘密鍵により暗号化する第１暗号化手段と、

前記位置情報又はその位置情報に関する情報を前記サブ公開鍵に対応するサブ秘密鍵により暗号化する第２暗号化手段とを有し、

前記復号化手段は、

前記マスタ秘密鍵に対応するマスタ公開鍵により前記暗号化されたソフト特徴情報と公開鍵系暗号関数のサブ公開鍵とを復号化する第１復号化手段と、

その復号化されたサブ公開鍵を用いて、前記暗号化された位置情報又はその位置情報に関する情報を復号化する第２復号化手段と、

を有していることを特徴とする請求項１５記載の再生装置。

１８．　前記位置情報書き込み手段は、少なくとも前記出力された位置情報又はその位置情報に関する情報についてディジタル署名を行うディジタル署名手段を有し、そのディジタル署名を行った結果に関する情報を前記ディスクに書き込み、

前記位置情報読み取り手段は、

前記ディジタル署名手段に対応する認証手段と、

その認証手段による認証過程から、及び／又は前記ディジタル署名結果に関する情報から前記位置情報を得る位置情報抽出手段とを有し、

前記比較判定手段は、前記認証手段により前記認証結果が正常である旨の出力がされた場合は、前記位置情報抽出手段により得られた位置情報と、前記マーキング読み取り手段による読み取り結果とを利用して、前記比較判定を行い、又、前記正常である旨の出力がされない場合は、前記再生を行わないことを特徴する請求項１４記載の再生装置。

１９．　前記ディジタル署名手段は、前記ディジタル署名する場合に、公開鍵系暗号関数の秘密鍵を用い、

前記認証手段は、前記秘密鍵に対応する公開鍵を用いて、前記認証を行うことを特徴する請求項１８記載の再生装置。

２０．　前記ディジタル署名手段手段は、

ディスクに書き込まれるソフト内容の特徴に関するソフト特徴情報と公開鍵系暗号関数のサブ公開鍵とについて、前記公開鍵系暗号関数のマスタ秘密鍵によりディジタル署名する第１ディジタル署名手段と、

前記位置情報又はその位置情報に関する情報について、前記サブ公開鍵に対応するサブ秘密鍵によりディジタル署名する第２ディジタル署名手段とを有し、

前記少なくとも前記出力された位置情報又はその位置情報に関する情報を書き込むとは、

前記第１ディジタル署名手段によるディジタル署名を行った結果に関する情報と、前記第２ディジタル署名手段によるディジタル署名を行った結果に関する情報とを前記ディスクに書き込むことであり、

前記位置情報読み取り手段は、

前記マスタ秘密鍵に対応するマスタ公開鍵により前記ディジタル署名された、ソフト特徴情報と公開鍵系暗号関数のサブ公開鍵とを認証する認証手段と、

その認証過程から、及び／又は前記ディジタル署名結果から得られたサブ公開鍵を用いて、前記認証過程から、及び／又は前記ディジタル署名結果から前記位置情報を得る位置情報抽出手段とを有し、

前記比較判定手段は、前記認証手段により前記認証結果が正常である旨の出力がされた場合は、前記位置情報抽出手段により得られた位置情報と、前記マーキング読み取り手段による読み取り結果とを利用して、前記比較判定を行い、又、前記正常である旨の出力がされない場合は、前記再生を行わないことを特徴とする請求項１８記載の再生装置。

２１．　前記比較判定の結果、前記位置情報読み取り手段による読み取り結果と、前記マーキング読み取り手段による読み取り結果とが相互に一致しない場合には、前記再生を行わないことを特徴する請求項１３～２０の何れか一つに記載の再生装置。

２２．　前記公開鍵系暗号関数は、ＲＳＡ関数又は楕円関数であることを特徴する請求項１６、１７、１９又は２０に記載の再生装置。

２３．　ディスクの成形を行うステップと、

前記成形されたディスクに反射膜を形成するステップと、

前記反射膜に対してマーキングを施すステップと、

前記マーキングの位置を検出するステップと、

前記検出された位置をマーキングの位置情報として出力し、暗号化して前記ディスクに書き込むステップと、

を備えたことを特徴する光ディスク製造方法。

２４．　ディスクの成形を行うステップと、

前記成形されたディスクに反射膜を形成するステップと、

前記反射膜に対してマーキングを施すステップと、

前記マーキングの位置を検出するステップと、

前記検出された位置をマーキングの位置情報として出力し、その位置情報に関連してディジタル署名して前記ディスクに書き込むステップと、

を備えたことを特徴する光ディスク製造方法。

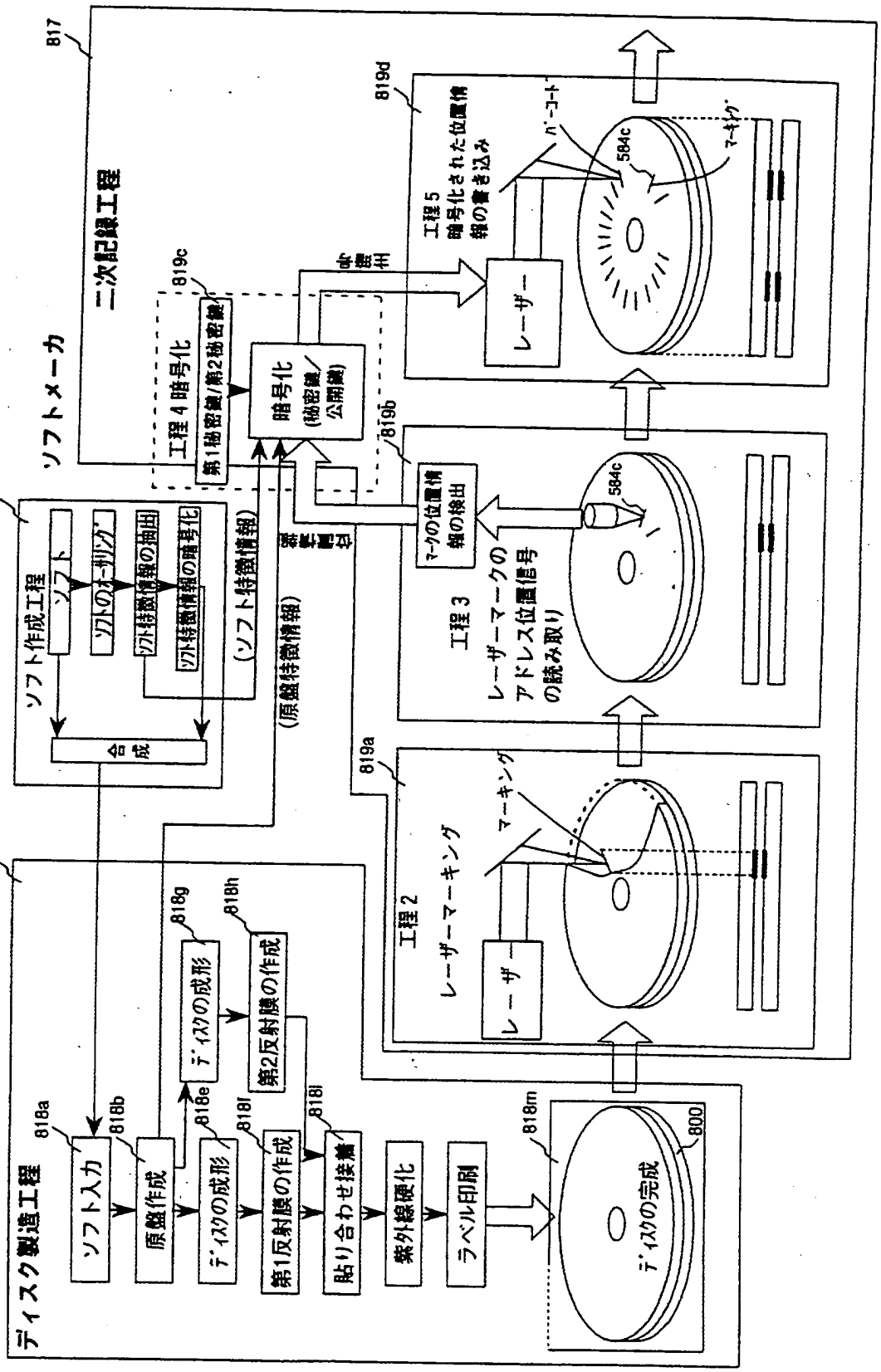
２５．　データの書き込まれたディスクの反射膜にレーザーによりマーキングが施されており、少なくともそのマーキングの位置情報又はその位置情報に関する情報が、暗号化され、あるいはディジタル署名された形で、前記ディスクに書き

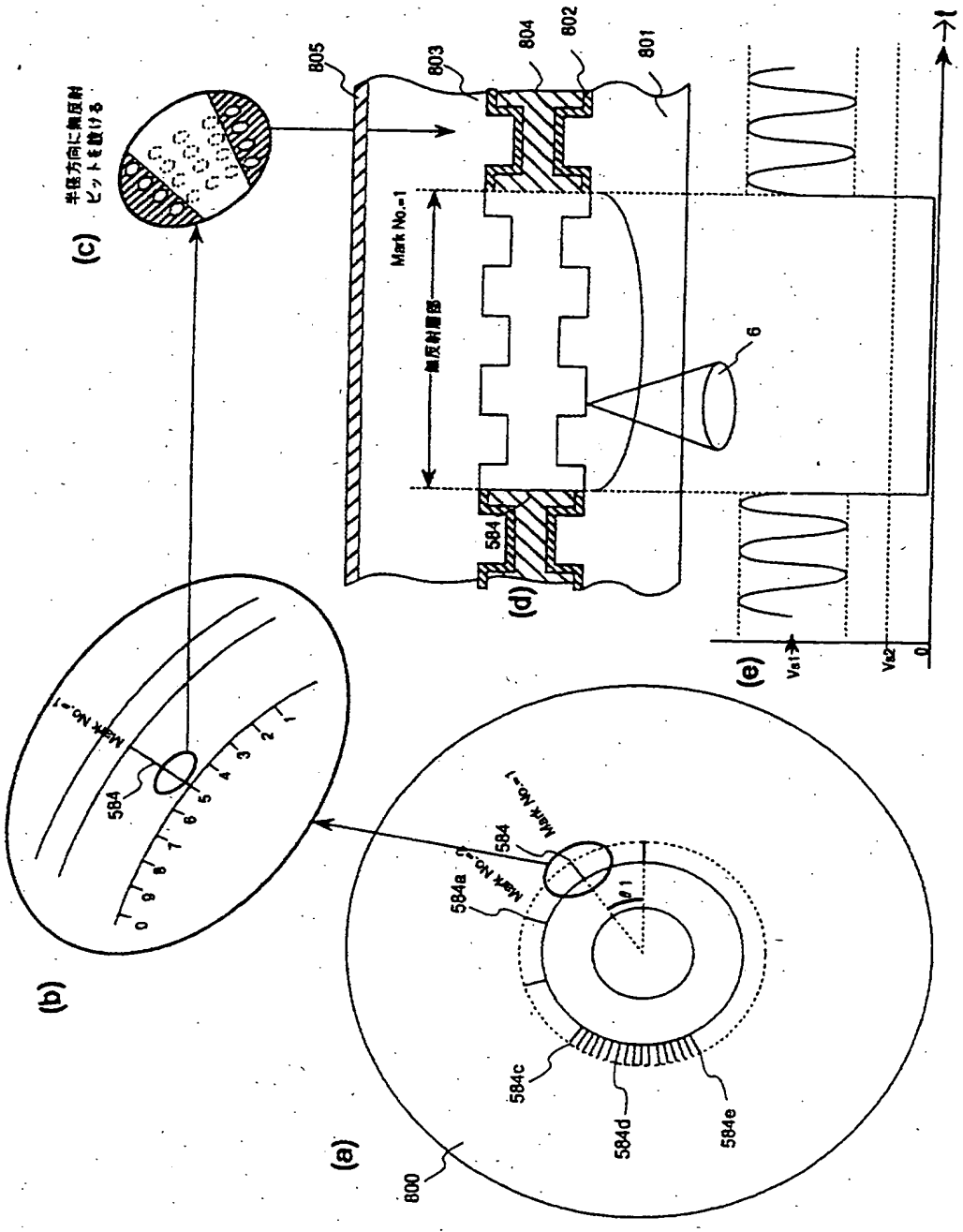
込まれていることを特徴とする光ディスク。

２６．　レーザにより消滅しない材料からなる２つの部材により反射膜が直接又は間接的に挟まれた構造を備えたディスクであって、その反射膜にレーザーによりマーキングが施されていることを特徴とする光ディスク。

２７．　ソフトコンテンツの特徴を、情報特徴抽出手段もしくは情報圧縮手段により、特徴抽出したソフト特徴情報と、前記ソフトコンテンツが海賊版防止もしくはコピー防止の対象ソフトであるか否かを示す海賊版防止識別子もしくはコピー防止識別子とを、一括して公開鍵系暗号関数の秘密鍵を用いてディジタル署名処理を行った結果の署名データが、前記ソフトコンテンツとともに、同一媒体上に記録されていることを特徴とする光ディスク。

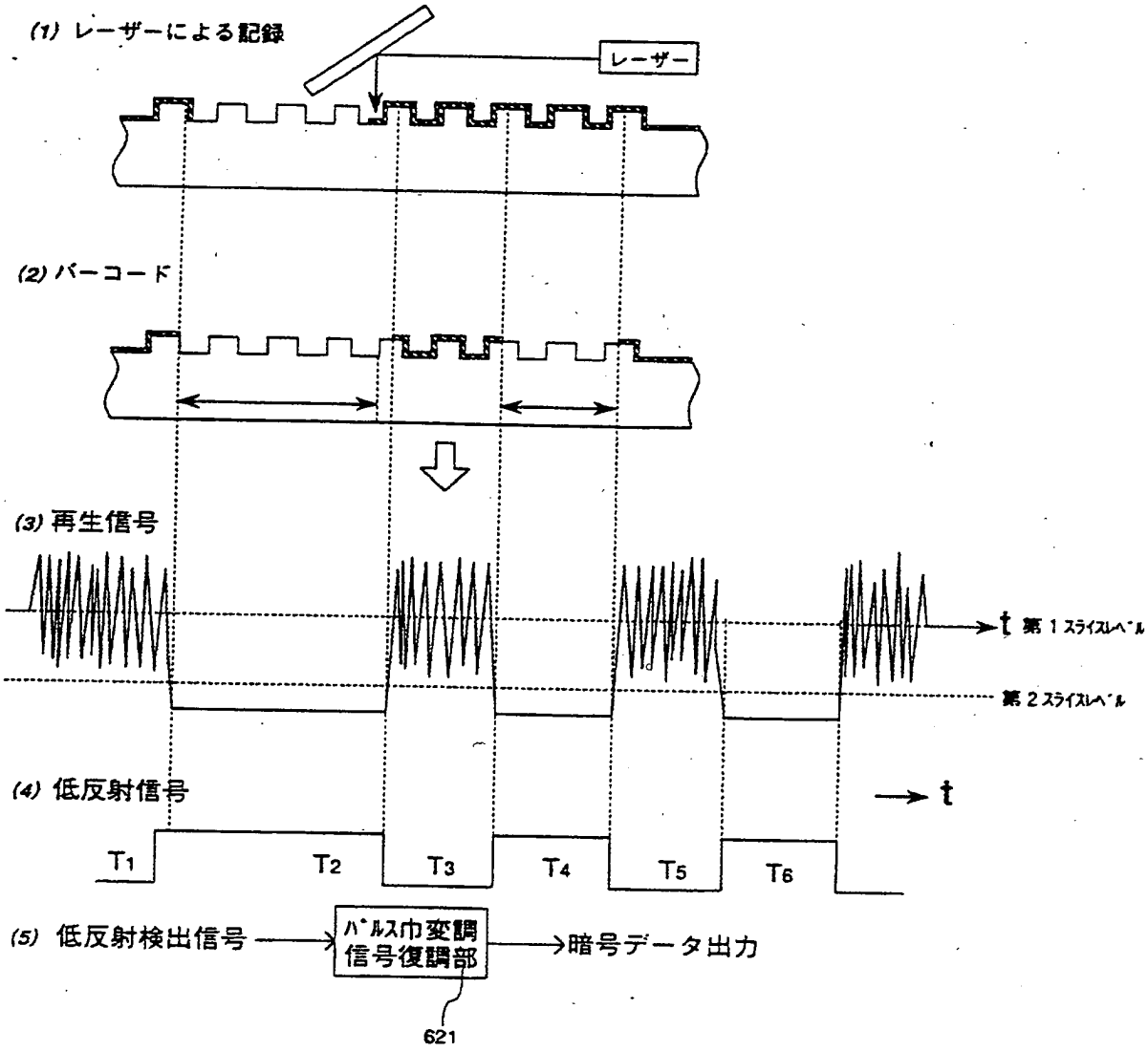
第1図


ディスク製造工程
ディスク工場
816
ソフトメーカ
817
二次記録工程
820
ソフト作成工程
ソフト
ソフトのチェック
ソフト特徴情報の抽出
ソフト特徴情報の暗号化
合成
(ソフト特徴情報)
(原盤特徴情報)
工程4 暗号化
第1秘密鍵/第2秘密鍵
819c
暗号化
(秘密鍵/公開鍵)
公開鍵
819b
マークの位置情報の検出
工程3
レーザーマークの
アドレス位置信号
の読み取り
584c
819a
工程2
レーザーマーキング
マーキング
レーザー
819d
工程5
暗号化された位置情報
の書き込み
レーザー
ピット
マーキング
584c
818a
ソフト入力
818b
原盤作成
818g
ディスクの成形
818e
ディスクの成形
818h
第2反射膜の作成
818f
第1反射膜の作成
818i
貼り合わせ接着
紫外線硬化
ラベル印刷
818m
ディスクの完成
800

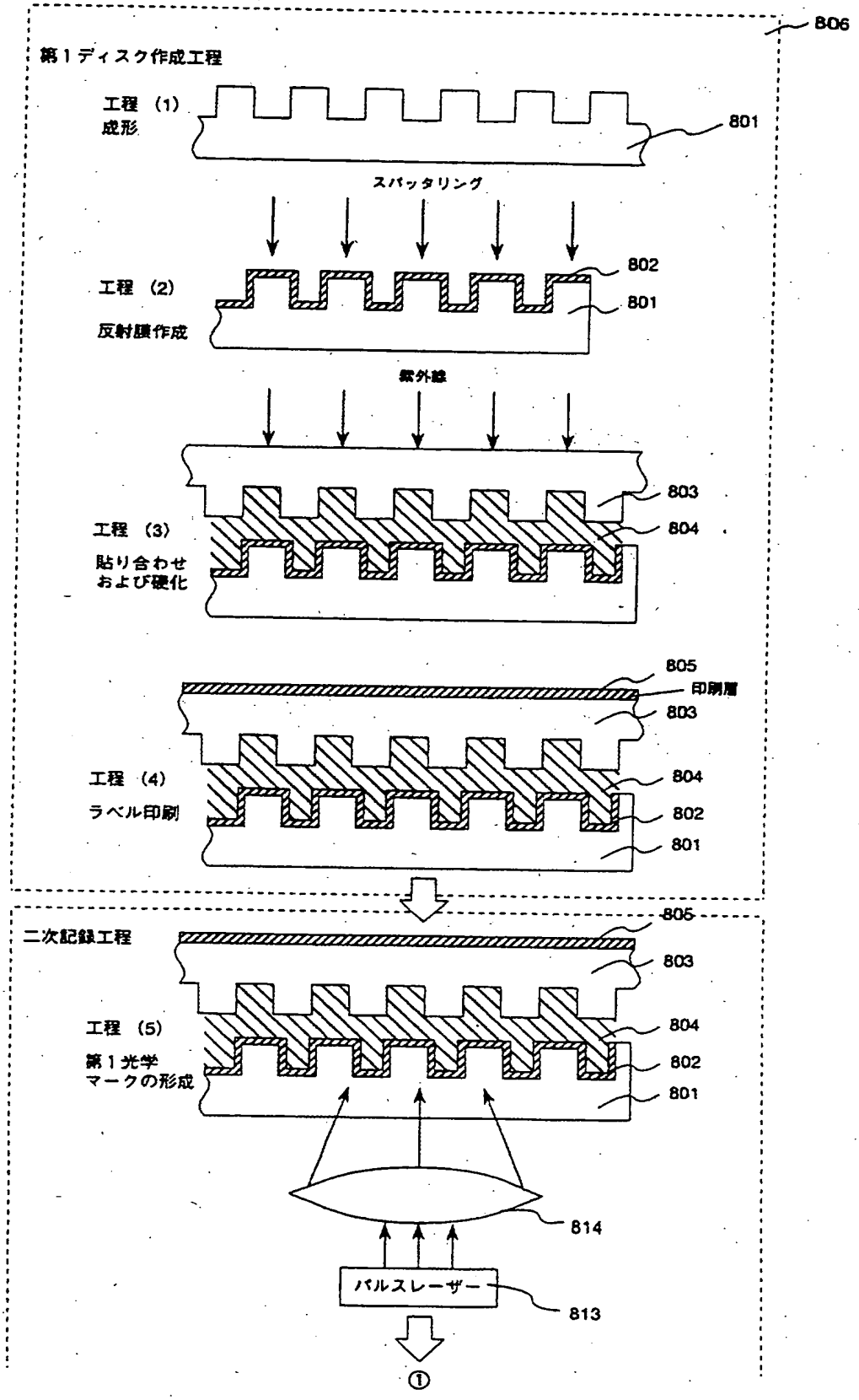

(a)
(b)
(c)
(d)
(e)
800
584
584a
584c
584d
584e
Mark No.=1
Mark No.=n
805
803
804
802
801
Mark No.=1
6
Vs1
Vs2
0
t

第2図

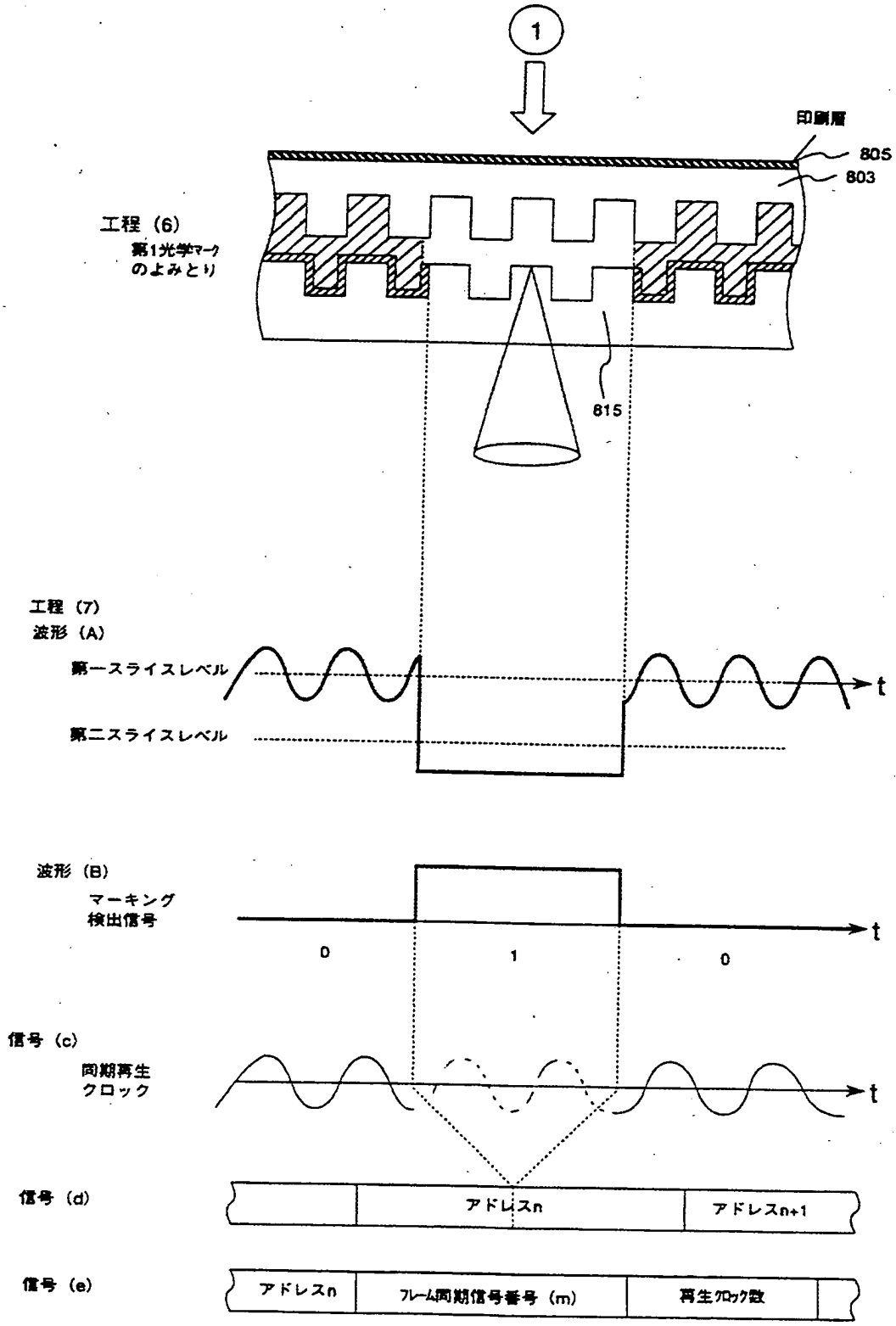
第３図


(1) レーザーによる記録
レーザー
(2) バーコード
(3) 再生信号
t 第１スライスレベル
第２スライスレベル
(4) 低反射信号
t
T1
T2
T3
T4
T5
T6
(5) 低反射検出信号
パルス巾変調
信号復調部
暗号データ出力
621

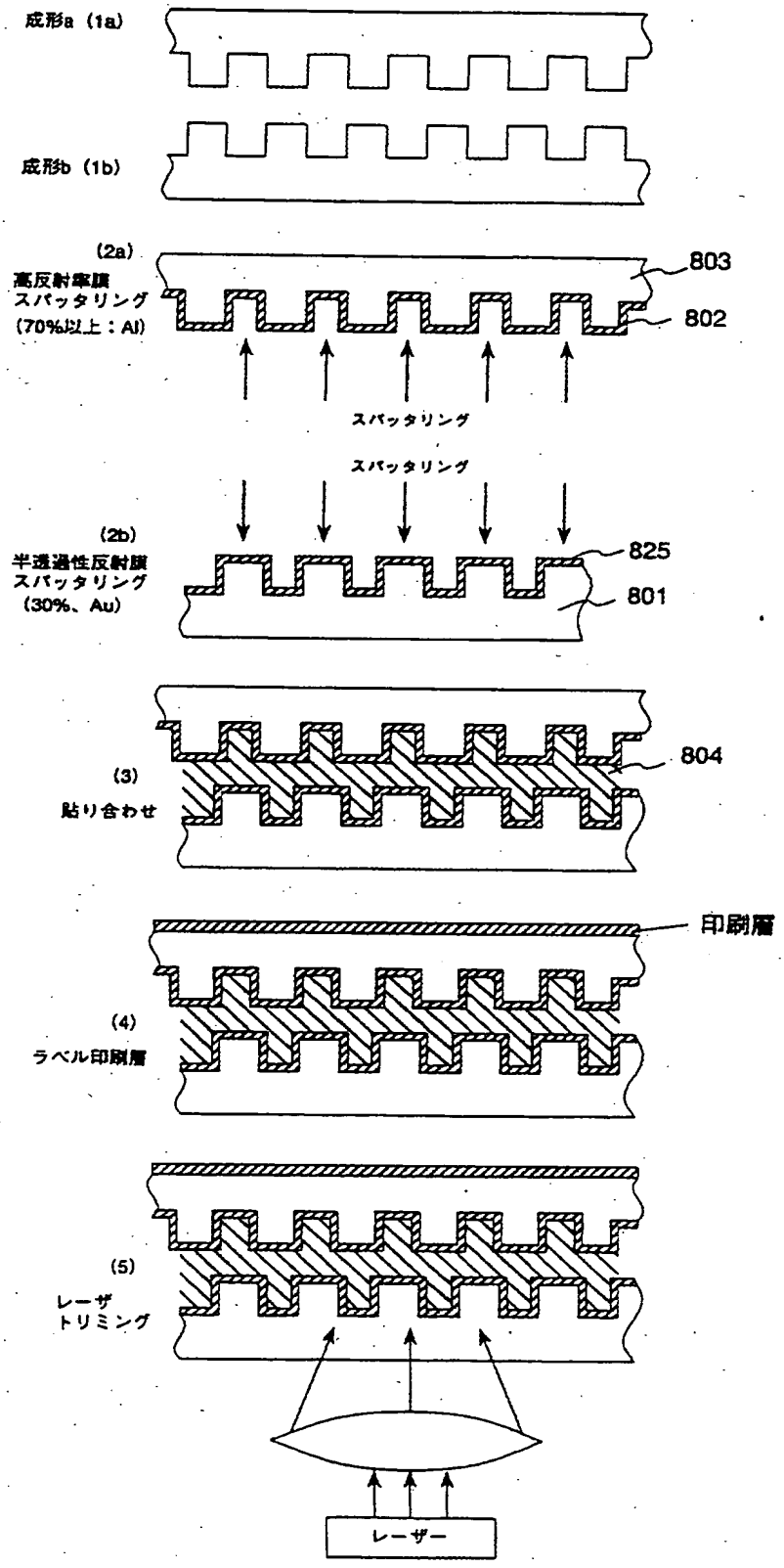
第4図


806
第1ディスク作成工程
工程 (1)
成形
801
スパッタリング
802
工程 (2)
801
反射膜作成
紫外線
803
工程 (3)
804
貼り合わせ
および硬化
805
印刷層
803
工程 (4)
804
ラベル印刷
802
801
二次記録工程
805
803
工程 (5)
804
第1光学
マークの形成
802
801
814
パルスレーザー
813
①

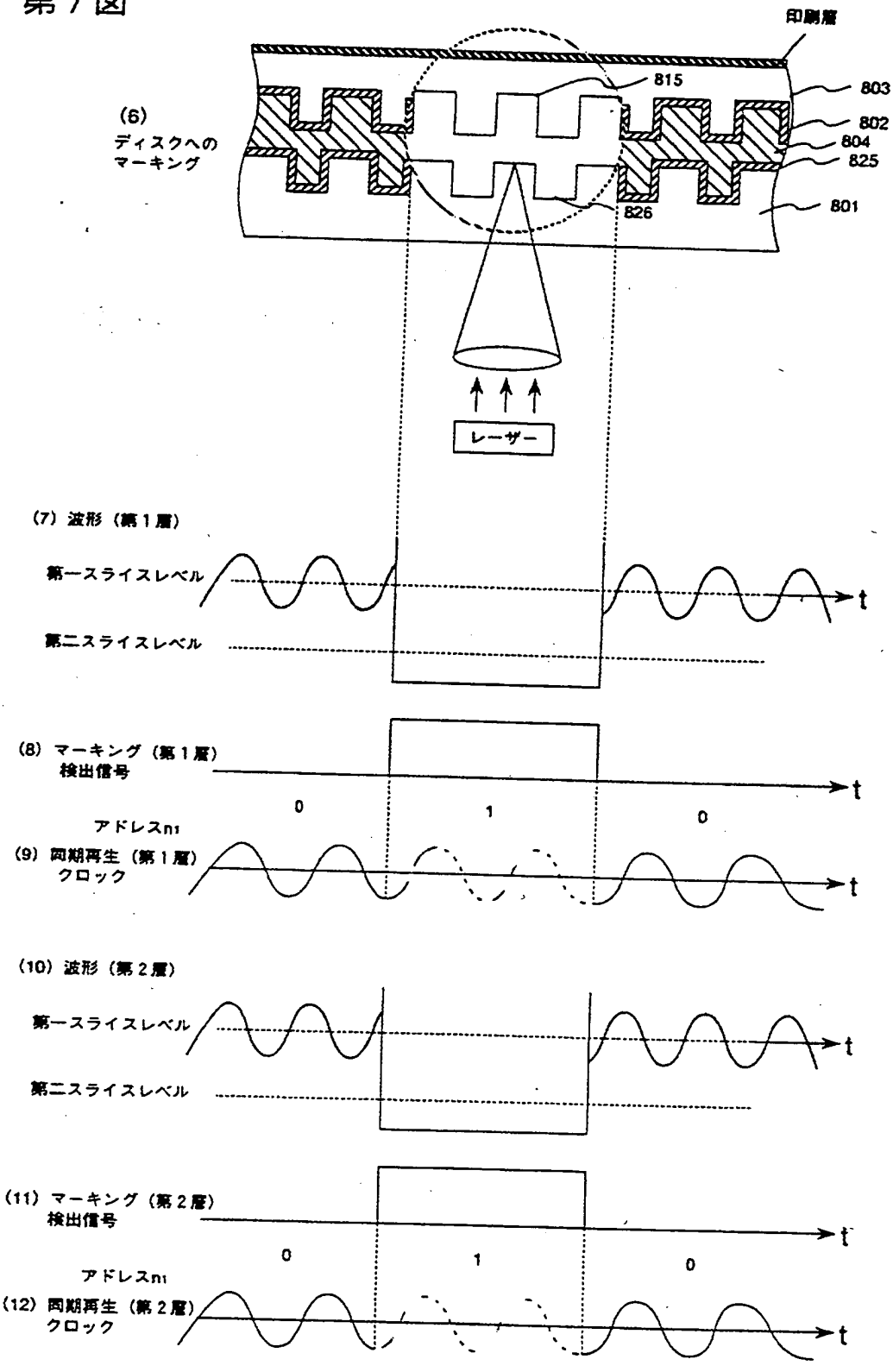
第5図


1
印刷層
805
803
工程 (6)
第1光学マーク
のよみとり
815
工程 (7)
波形 (A)
第一スライスレベル
第二スライスレベル
t
波形 (B)
マーキング
検出信号
0
1
0
t
信号 (c)
同期再生
クロック
t
信号 (d)
アドレスn
アドレスn+1
信号 (e)
アドレスn
フレーム同期信号番号 (m)
再生クロック数

第6図

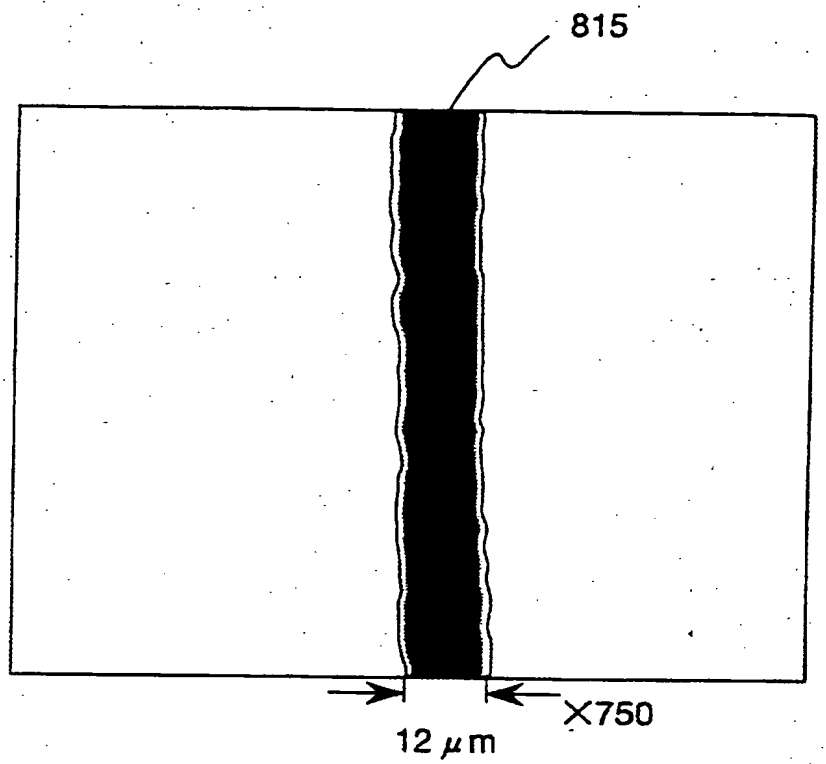

成形a (1a)
成形b (1b)
(2a)
高反射率膜
スパッタリング
(70%以上：Al)
803
802
スパッタリング
スパッタリング
(2b)
半透過性反射膜
スパッタリング
(30%、Au)
825
801
(3)
貼り合わせ
804
印刷層
(4)
ラベル印刷層
(5)
レーザ
トリミング
レーザー

第７図

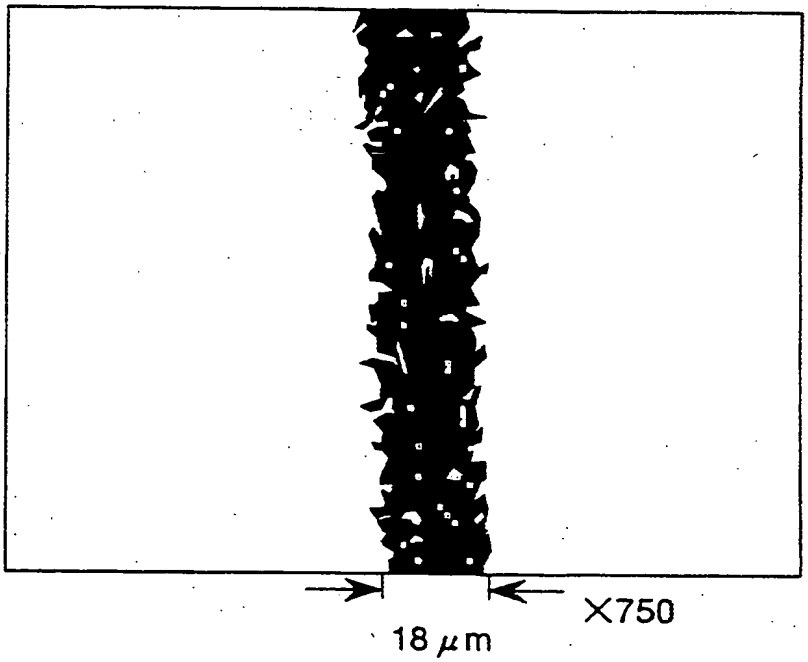

(6)
ディスクへの
マーキング
印刷層
815
803
802
804
825
826
801
レーザー
(7) 波形（第１層）
第一スライスレベル
第二スライスレベル
t
(8) マーキング（第１層）
検出信号
0
1
0
アドレスn1
(9) 同期再生（第１層）
クロック
(10) 波形（第２層）
第一スライスレベル
第二スライスレベル
(11) マーキング（第２層）
検出信号
アドレスn1
(12) 同期再生（第２層）
クロック

第８図

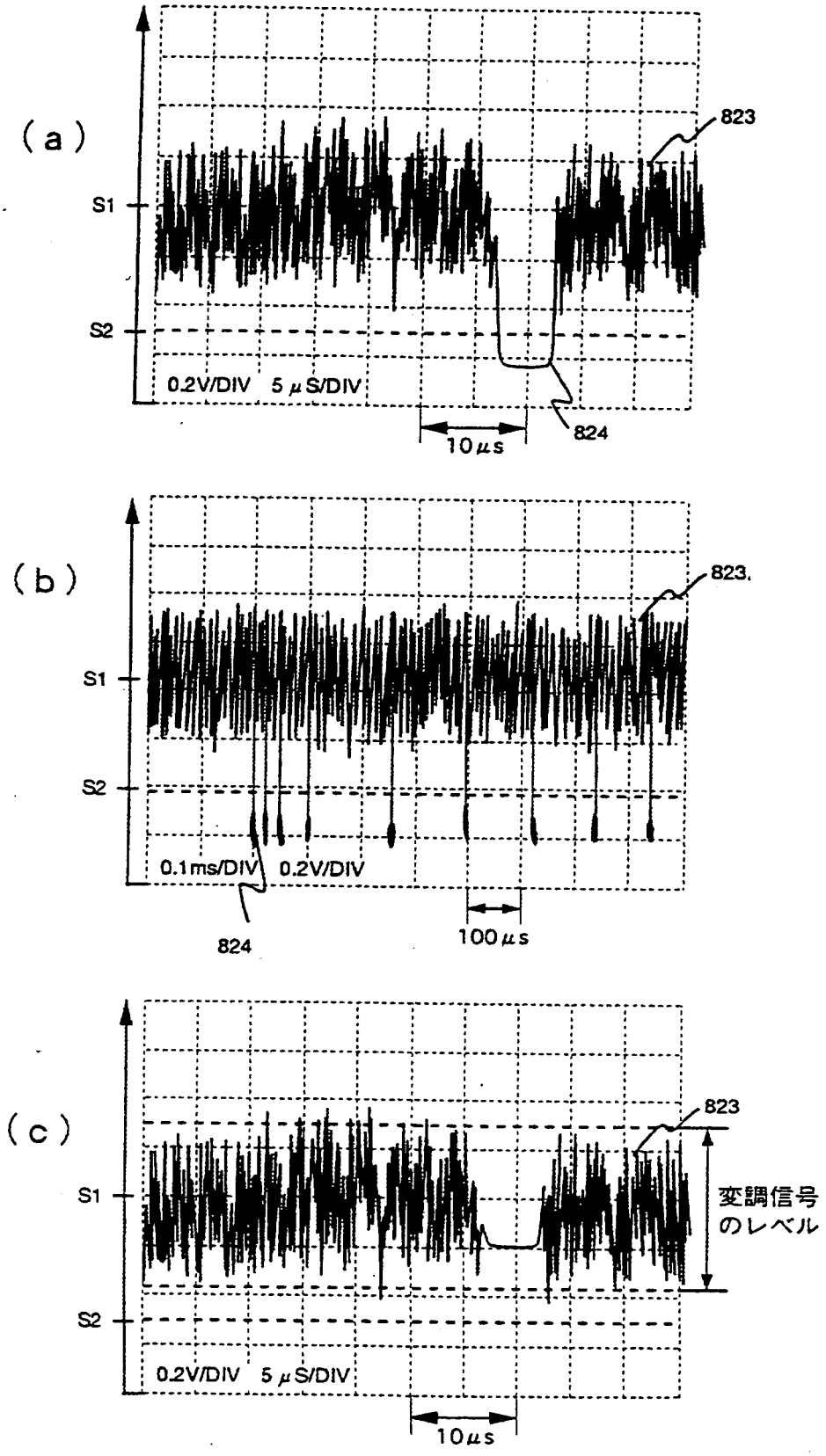
(a)



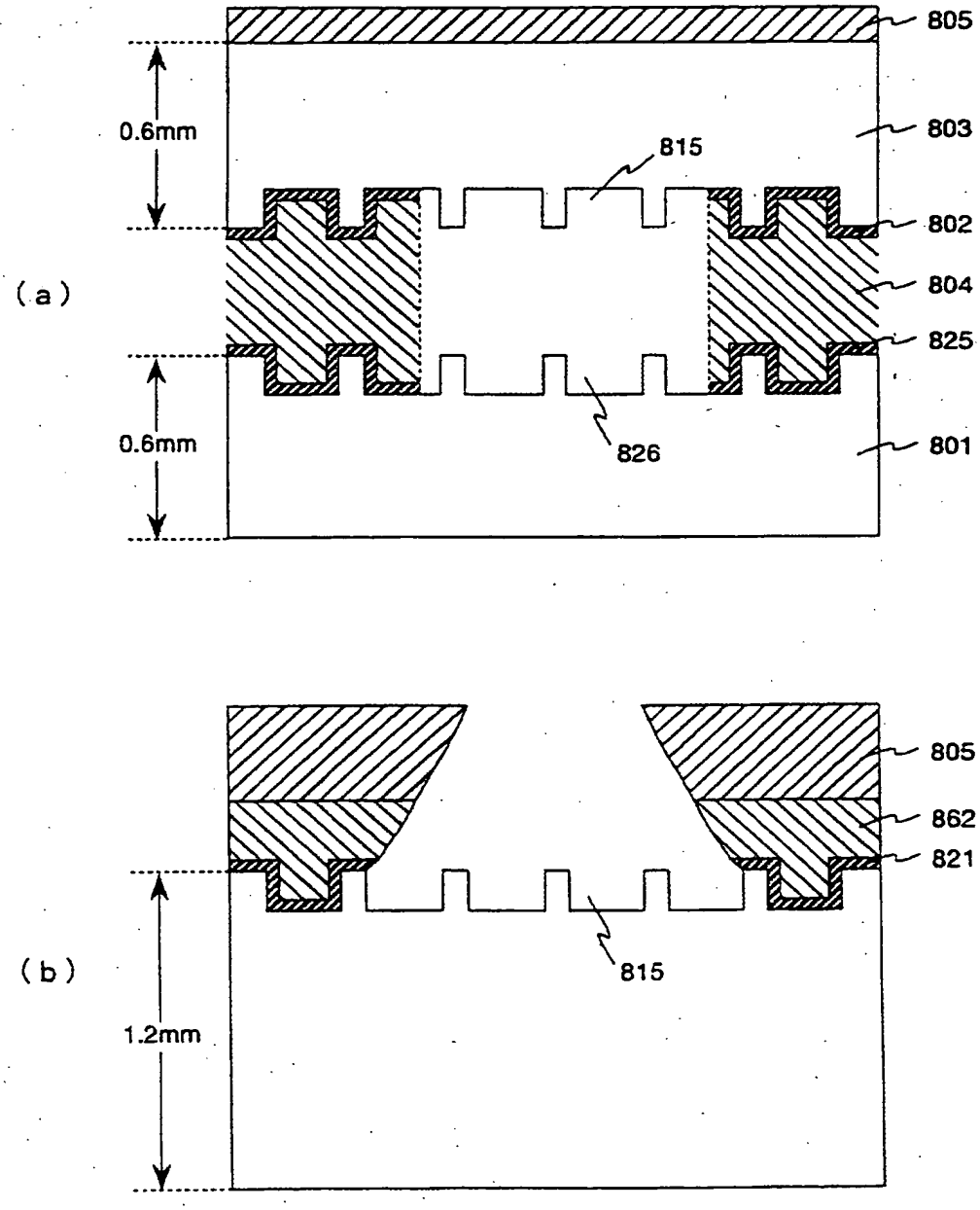
(b)



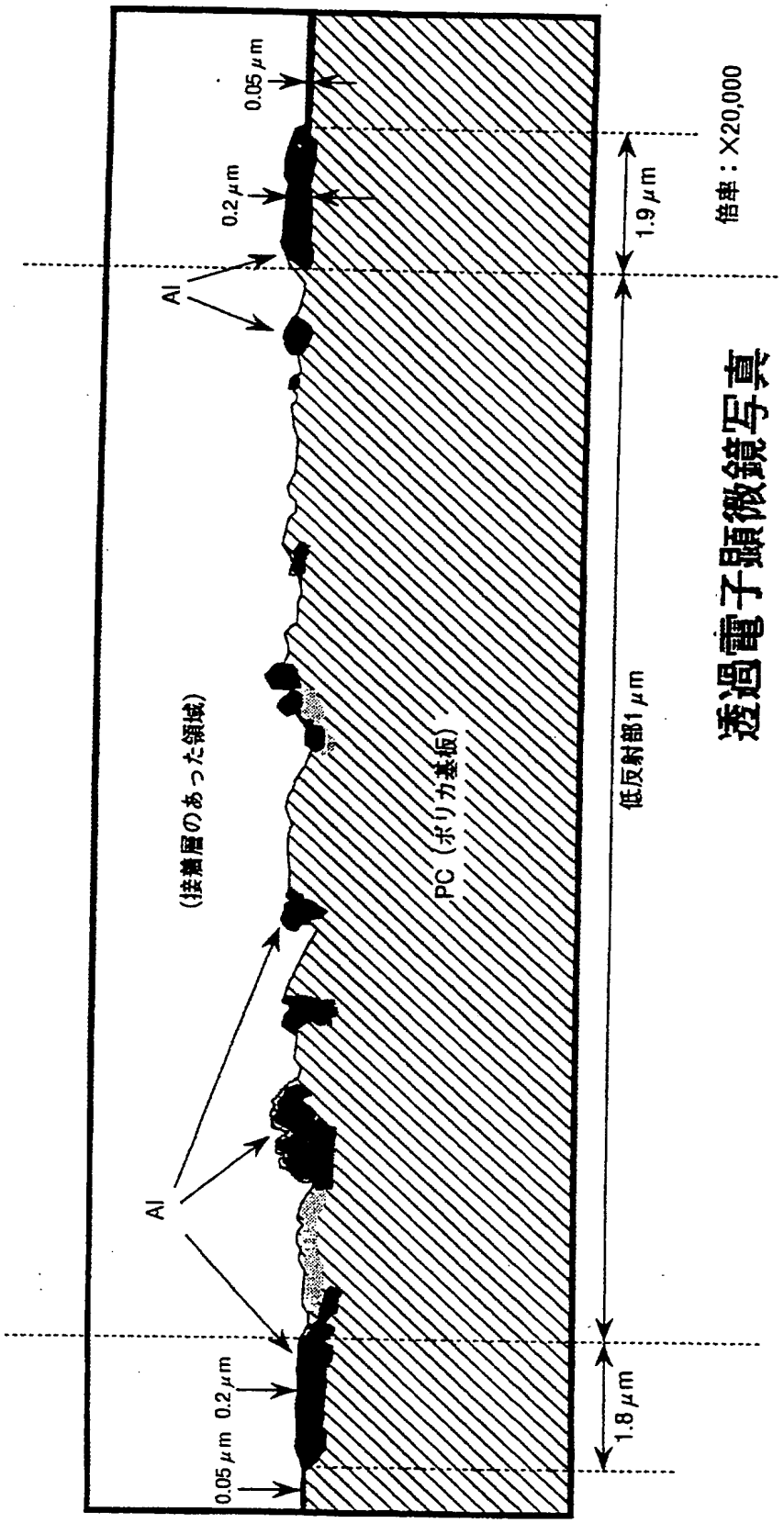
第９図


(a)
S1
S2
823
824
0.2V/DIV 5μS/DIV
10μs
(b)
S1
S2
823
824
0.1ms/DIV 0.2V/DIV
100μs
(c)
S1
S2
823
変調信号
のレベル
0.2V/DIV 5μS/DIV
10μs

第１０図

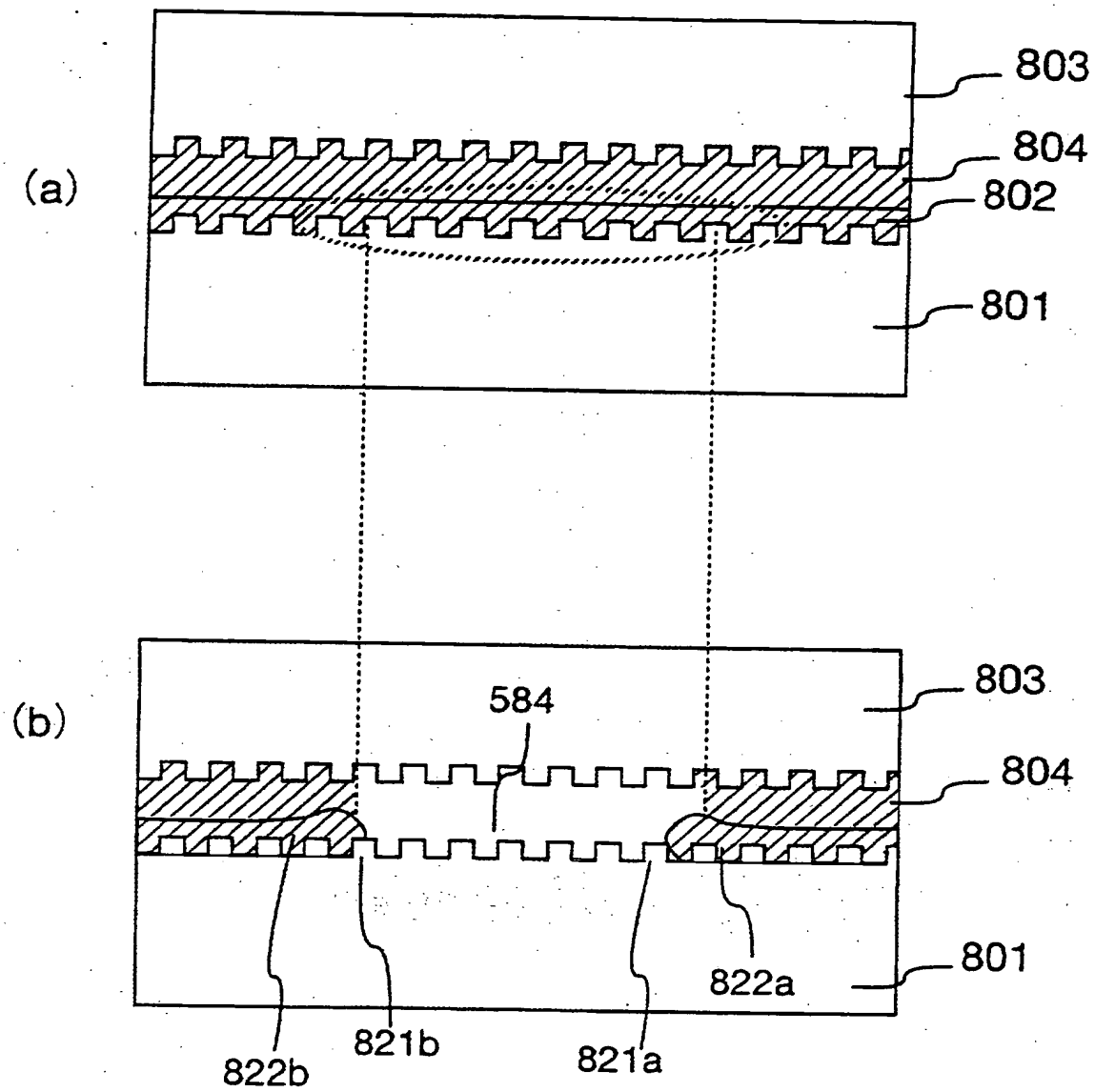

(a)
805
803
815
802
804
825
826
801
0.6mm
0.6mm
(b)
805
862
821
815
1.2mm

第１１図

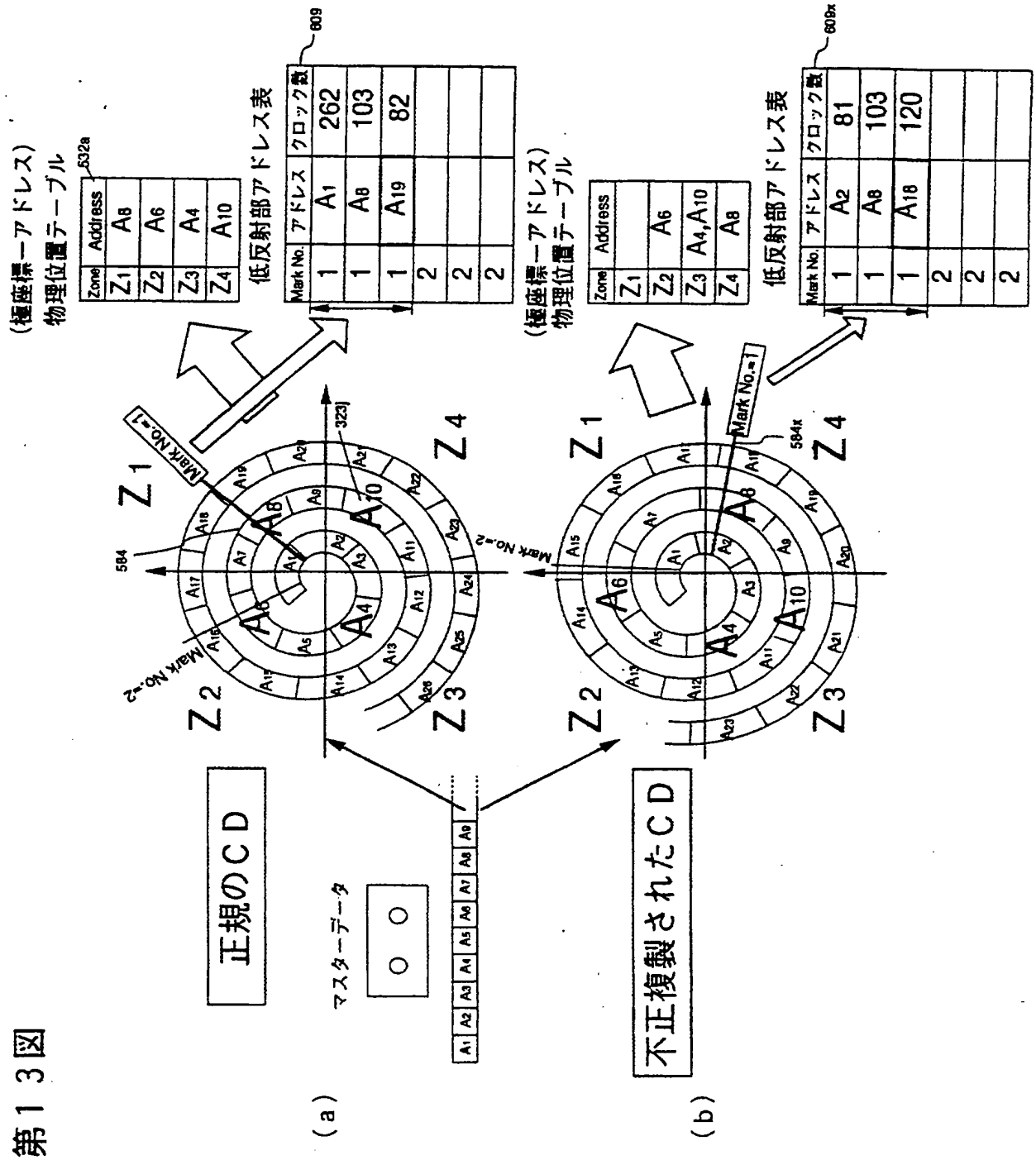


透過電子顕微鏡写真

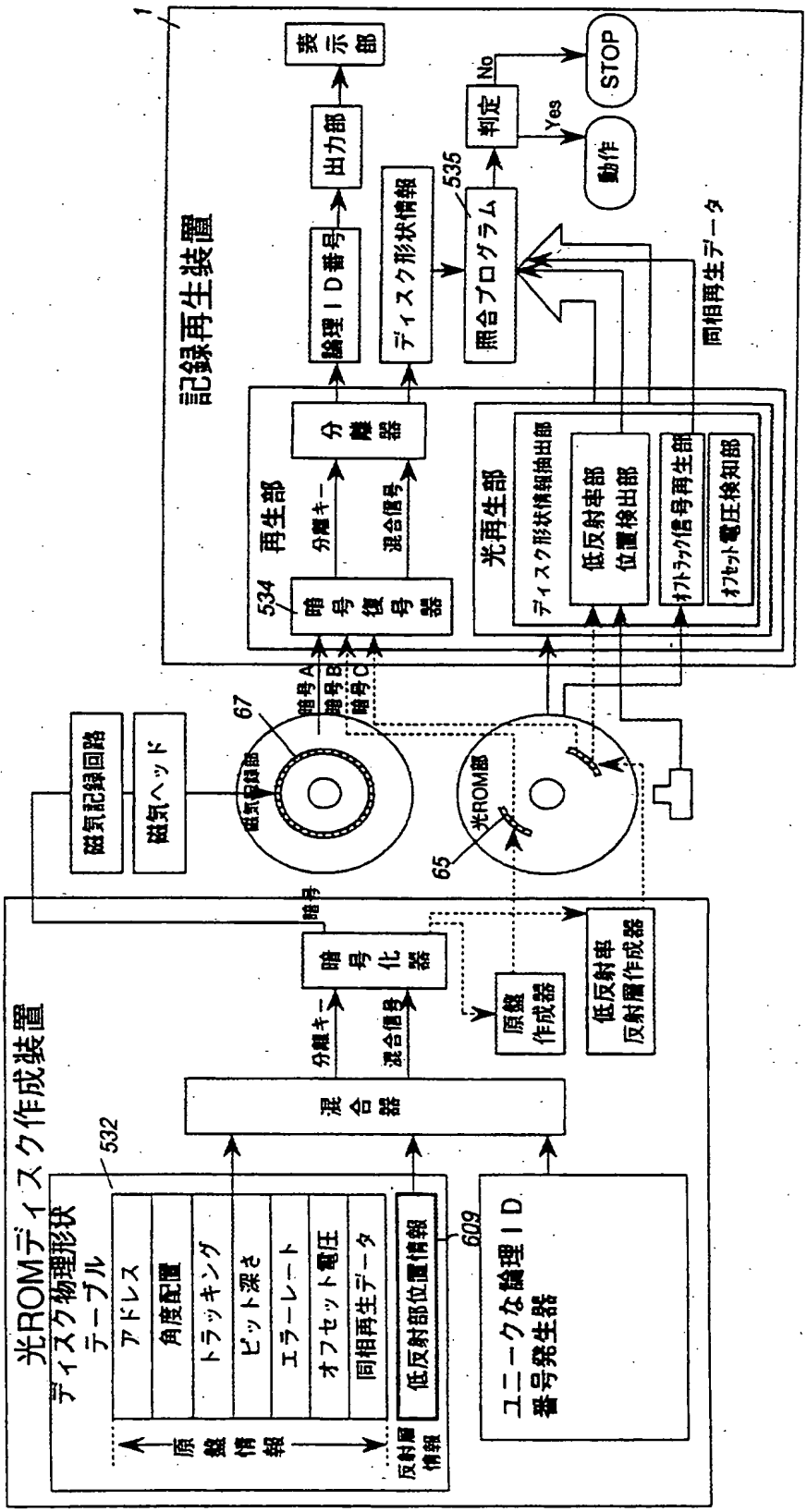
第１２図



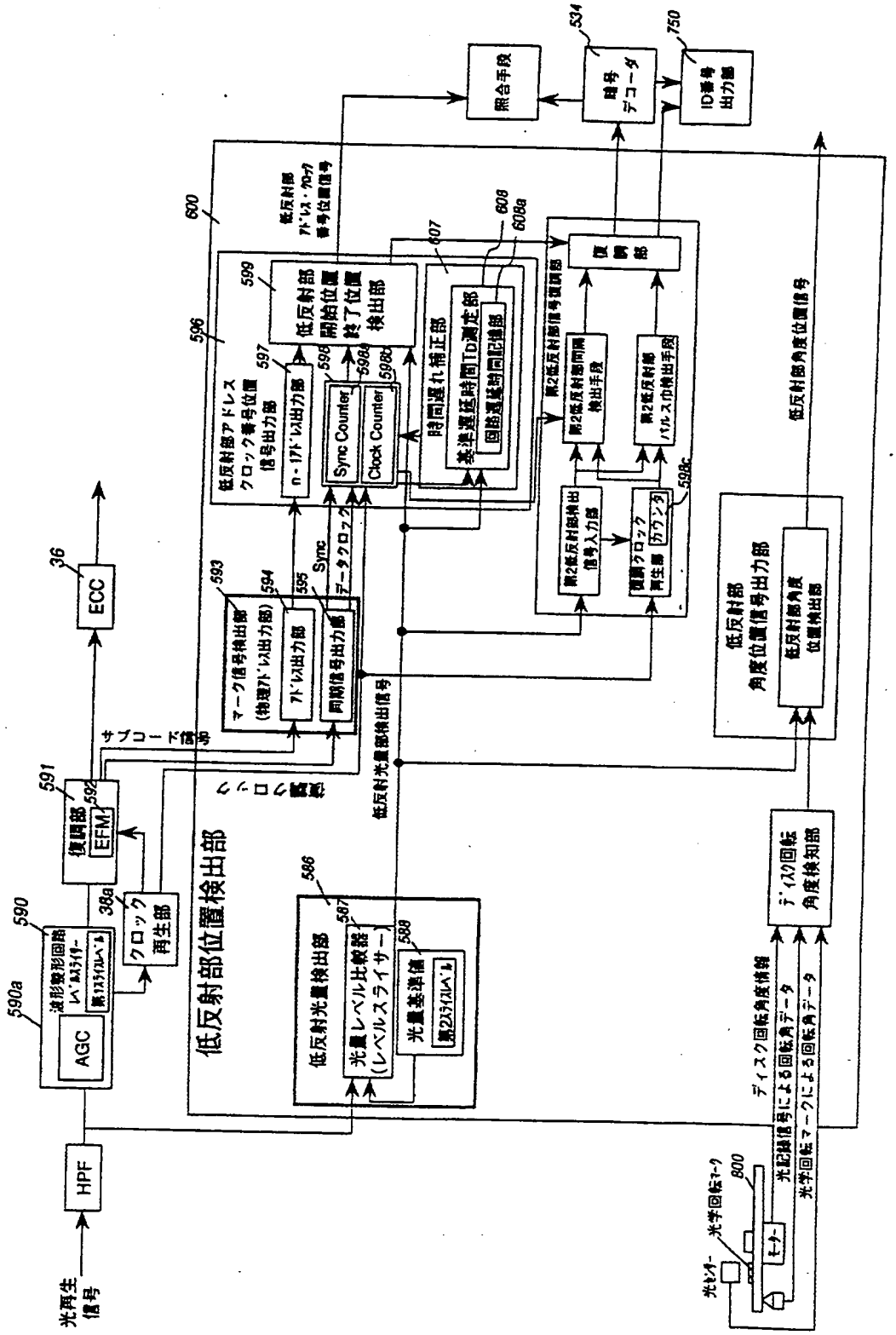
第１３図


(極座標－アドレス)
物理位置テーブル
Zone
Address
Z1 A8
Z2 A6
Z3 A4
Z4 A10
低反射部アドレス表
Mark No.
アドレス
クロック数
1 A1 262
1 A8 103
1 A19 82
2
2
2
Mark No.=1
Mark No.=2
Z1
Z2
Z3
Z4
正規のCD
マスターデータ
○ ○
(a)
(極座標－アドレス)
物理位置テーブル
Zone
Address
Z1
Z2 A6
Z3 A4,A10
Z4 A8
低反射部アドレス表
Mark No.
アドレス
クロック数
1 A2 81
1 A8 103
1 A18 120
2
2
2
不正複製されたCD
(b)

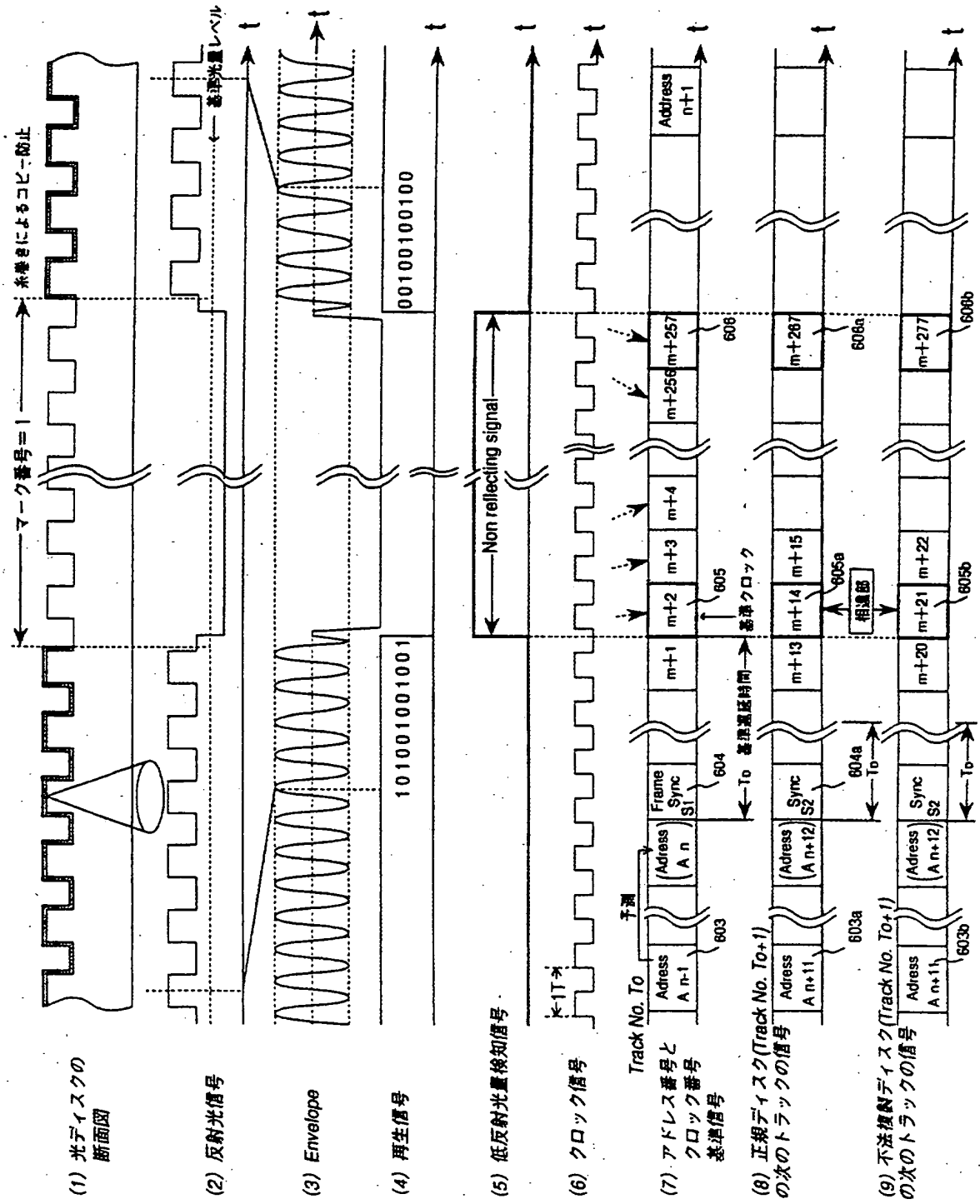
第１４図


光ROMディスク作成装置
ディスク物理形状テーブル
532
アドレス
角度配置
トラッキング
ピット深さ
エラーレート
オフセット電圧
同相再生データ
低反射部位置情報
609
原盤情報
反射層情報
ユニークな論理ＩＤ番号発生器
混合器
分離キー
混合信号
暗号化器
原盤作成器
低反射率反射層作成器
暗号
磁気記録回路
磁気ヘッド
67
暗号A
暗号B
暗号C
磁気記録部
光ROM部
65
記録再生装置
1
再生部
534
暗号復号器
分離器
光再生部
ディスク形状情報抽出部
低反射率部位置検出部
オフトラック信号再生部
オフセット電圧検知部
論理ＩＤ番号
ディスク形状情報
照合プログラム
535
出力部
表示部
判定
No
Yes
STOP
動作
同相再生データ

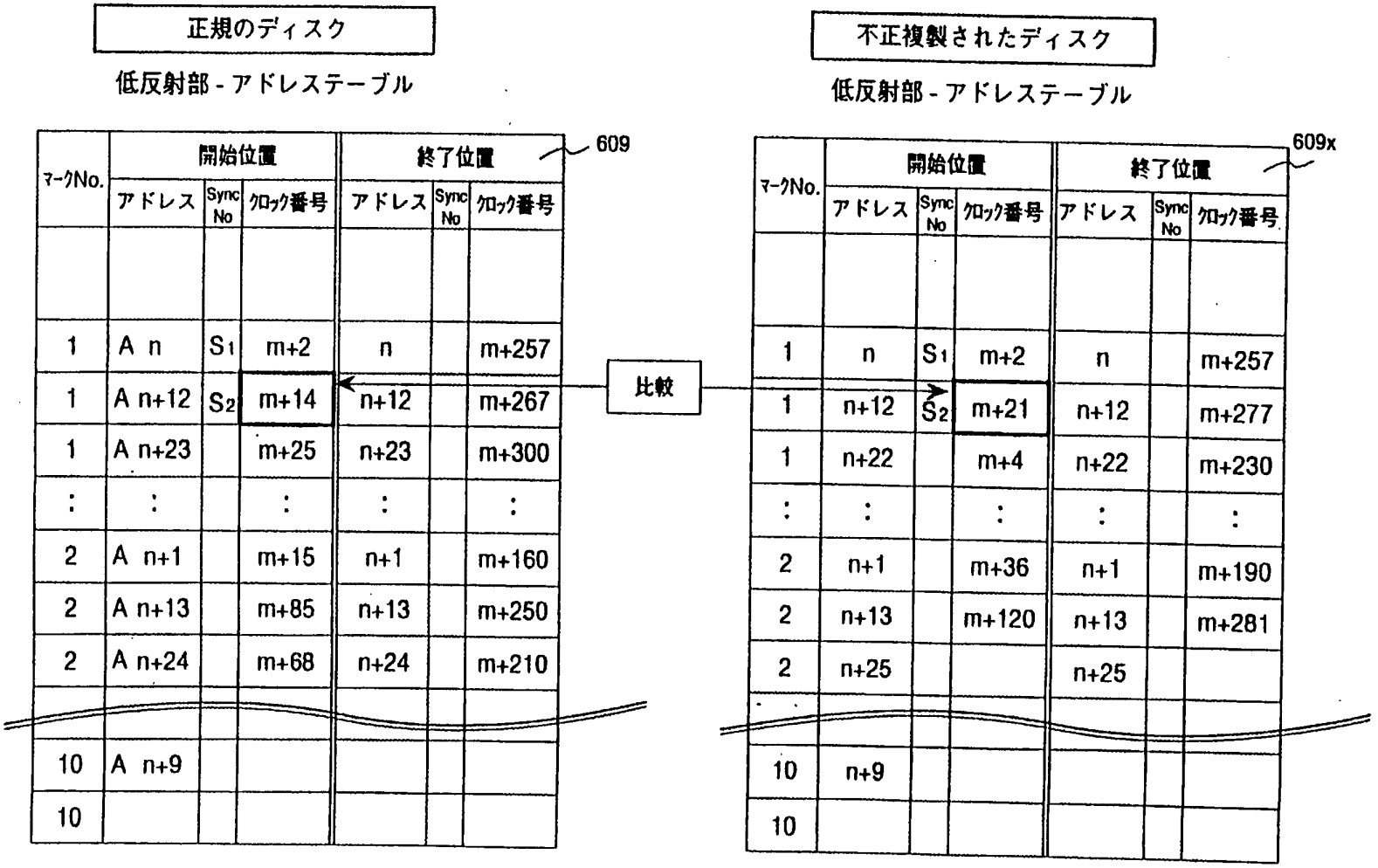
第１５図


光再生信号
HPF
590a
波形整形回路
AGC
第1スライスレベル
590
38a
クロック再生部
591
復調部
EFM
592
サブコード
36
ECC
低反射部位置検出部
586
低反射光量検出部
587
光量レベル比較器
(レベルスライサー)
588
光量基準値
第2スライスレベル
低反射光量検出信号
クロック
593
マーク信号検出部
(物理アドレス出力部)
594
アドレス出力部
595
同期信号出力部
Sync
データクロック
600
596
低反射部アドレス
クロック番号位置
信号出力部
597
n-17アドレス出力部
598
Sync Counter
598a
Clock Counter
598b
599
低反射部
開始位置
終了位置
検出部
低反射部
アドレス・カウント
番号位置信号
607
時間遅れ補正部
基準遅延時間TD測定部
回路遅延時間記憶部
608
608a
復調部
第2低反射部信号復調部
第2低反射部信号
入力部
598c
復調クロック
再生部
カウンタ
第2低反射部
同期
検出手段
第2低反射部
パルス中検出手段
低反射部
角度位置信号出力部
低反射部
位置検出部
低反射部角度位置信号
照合手段
534
暗号
デコーダ
750
ID番号
出力部
ディスク回転
角度検知部
ディスク回転角度情報
光記録信号による回転角データ
光学回転マークによる回転角データ
光センサー
光学回転マーク
800
モーター

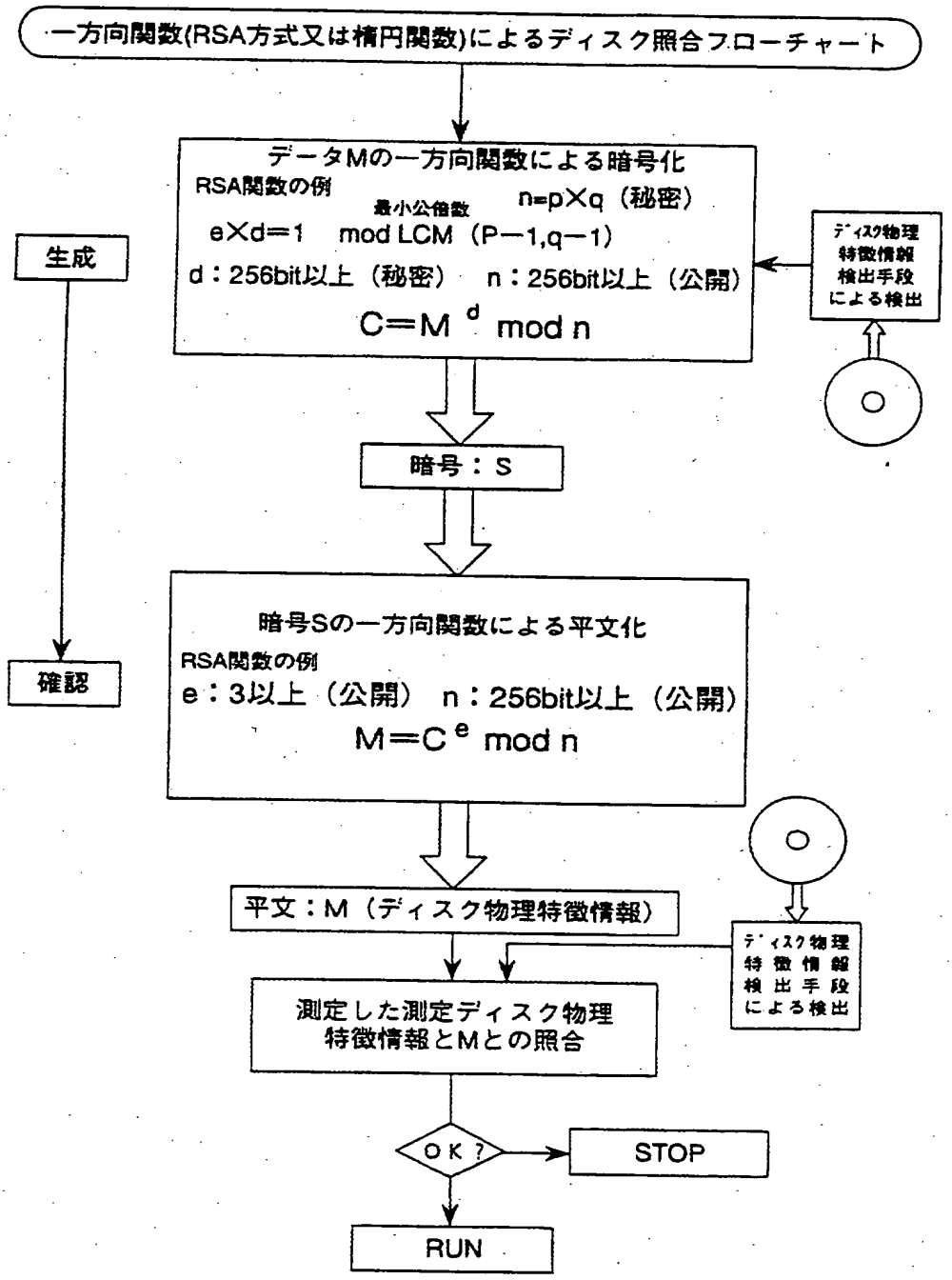
第16図


(1) 光ディスクの断面図
マーク番号=1
未使用によるコピー防止
(2) 反射光信号
基準光量レベル
(3) Envelope
(4) 再生信号
0010010010 0
(5) 低反射光量検知信号
Non reflecting signal
(6) クロック信号
1T
(7) アドレス番号とクロック番号基準信号
Track No. To
予測
Adress A n-1
Adress A n
Frame Sync S1
m+1
m+2
m+3
m+4
m+256
m+257
Address n+1
603
604
605
606
To 基準遅延時間
基準クロック
(8) 正規ディスク(Track No. To+1)の次のトラックの信号
Adress A n+11
Adress A n+12
Sync S2
m+13
m+14
m+15
m+287
603a
604a
605a
606a
相違部
(9) 不法複製ディスク(Track No. To+1)の次のトラックの信号
Adress A n+11
Adress A n+12
Sync S2
m+20
m+21
m+22
m+277
603b
604a
605b
606b
To
t

第１７図


正規のディスク
低反射部 - アドレステーブル
609
マークNo.
開始位置
アドレス
Sync No
クロック番号
終了位置
アドレス
Sync No
クロック番号
1 A n S1 m+2 n m+257
1 A n+12 S2 m+14 n+12 m+267
1 A n+23 m+25 n+23 m+300
: : : : :
2 A n+1 m+15 n+1 m+160
2 A n+13 m+85 n+13 m+250
2 A n+24 m+68 n+24 m+210
10 A n+9
10
比較
不正複製されたディスク
低反射部 - アドレステーブル
609x
1 n S1 m+2 n m+257
1 n+12 S2 m+21 n+12 m+277
1 n+22 m+4 n+22 m+230
: : : : :
2 n+1 m+36 n+1 m+190
2 n+13 m+120 n+13 m+281
2 n+25 n+25
10 n+9
10

第１８図


一方向関数(RSA方式又は楕円関数)によるディスク照合フローチャート
データMの一方向関数による暗号化
RSA関数の例
最小公倍数
n=p×q（秘密）
e×d=1 mod LCM（P−1,q−1）
d：256bit以上（秘密） n：256bit以上（公開）
C=M d mod n
生成
ディスク物理特徴情報検出手段による検出
暗号：S
暗号Sの一方向関数による平文化
RSA関数の例
e：3以上（公開） n：256bit以上（公開）
M=C e mod n
確認
平文：M（ディスク物理特徴情報）
ディスク物理特徴情報検出手段による検出
測定した測定ディスク物理特徴情報とMとの照合
OK？
STOP
RUN

第19図

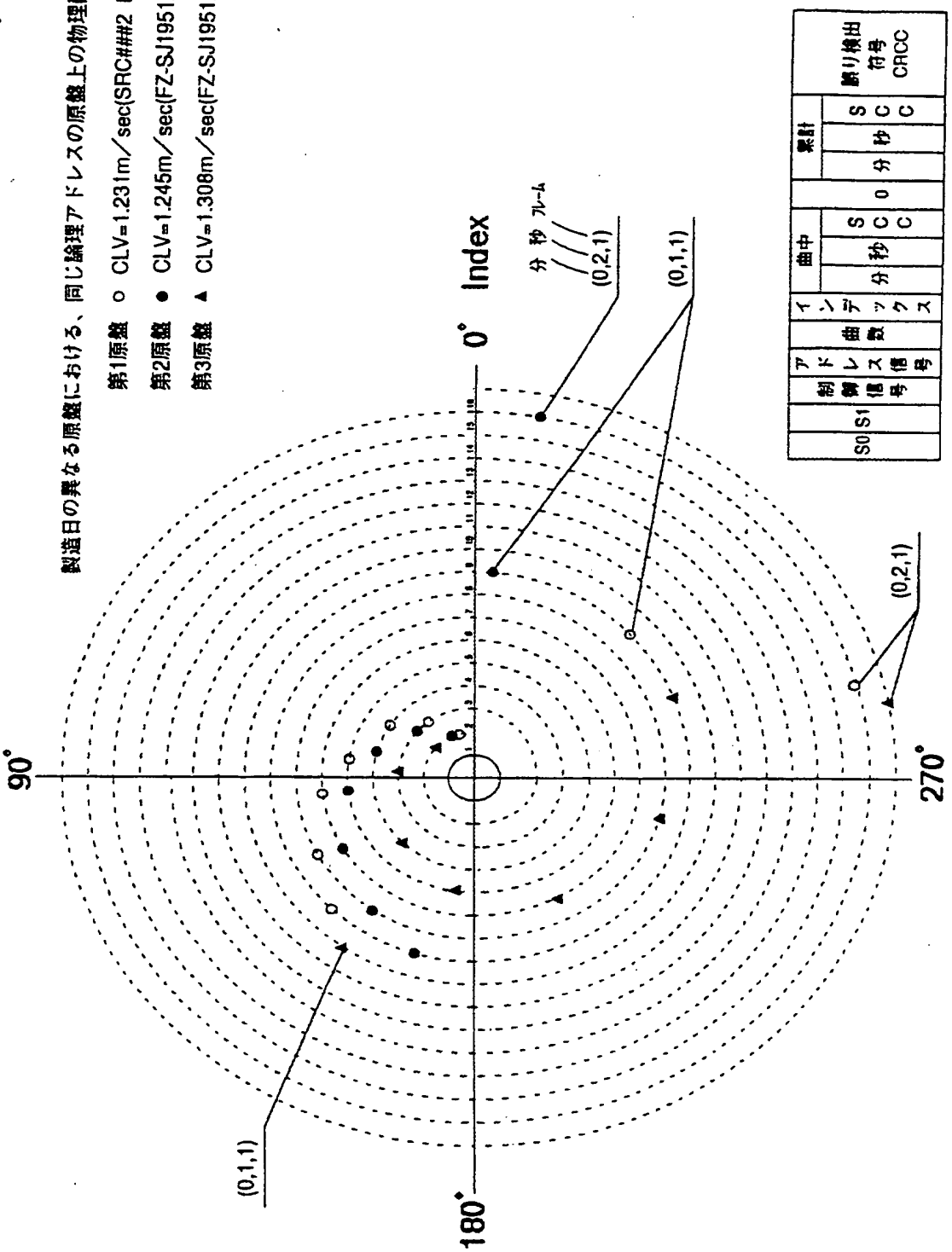
論理アドレスの物理的位置が原盤毎により異なることを示す図

製造日の異なる原盤における、同じ論理アドレスの原盤上の物理配置点

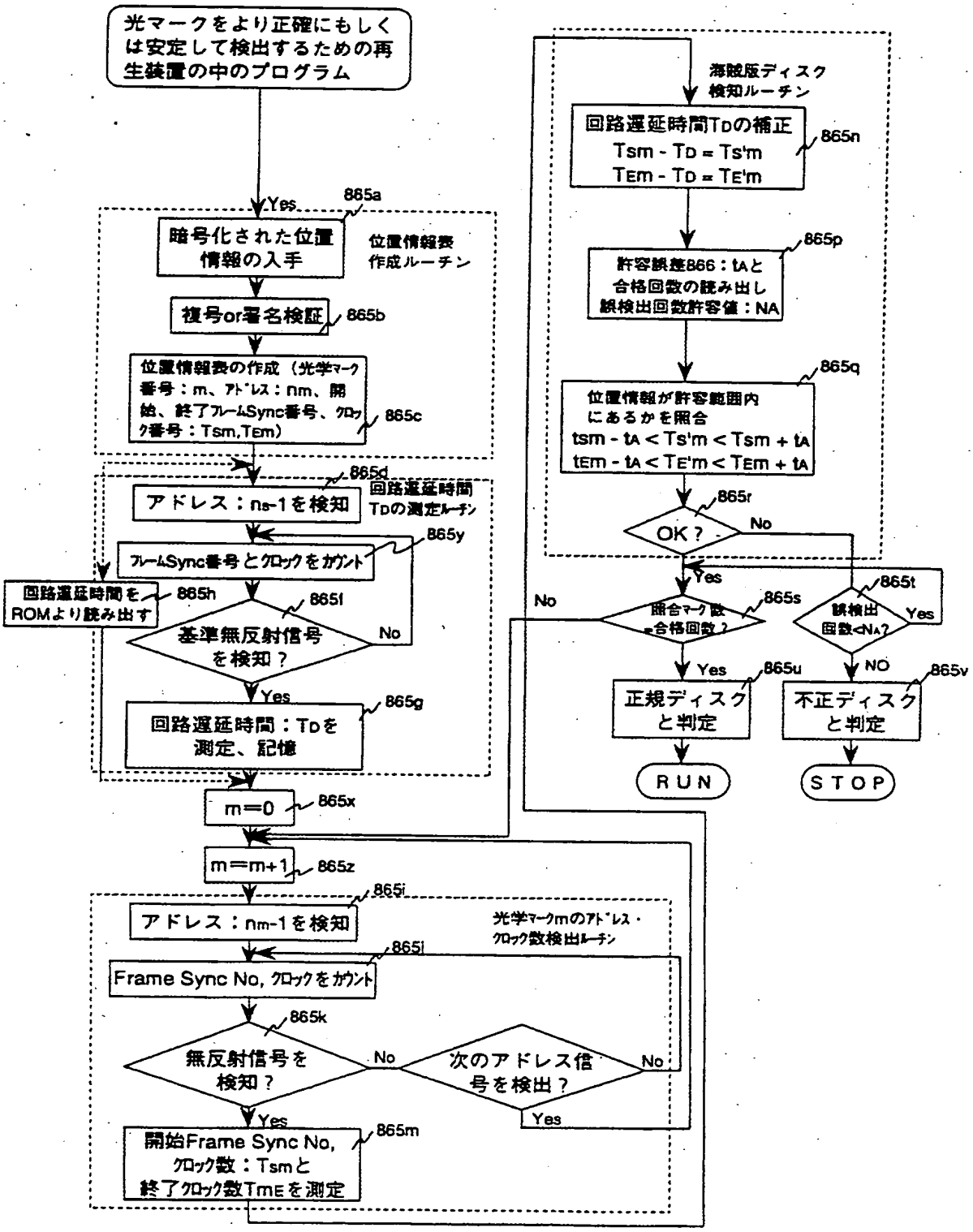
第1原盤 ○ CLV=1.231m／sec(SRC#ﾊﾝ#2 MISI)

第2原盤 ● CLV=1.245m／sec(FZ-SJ1951A 3)

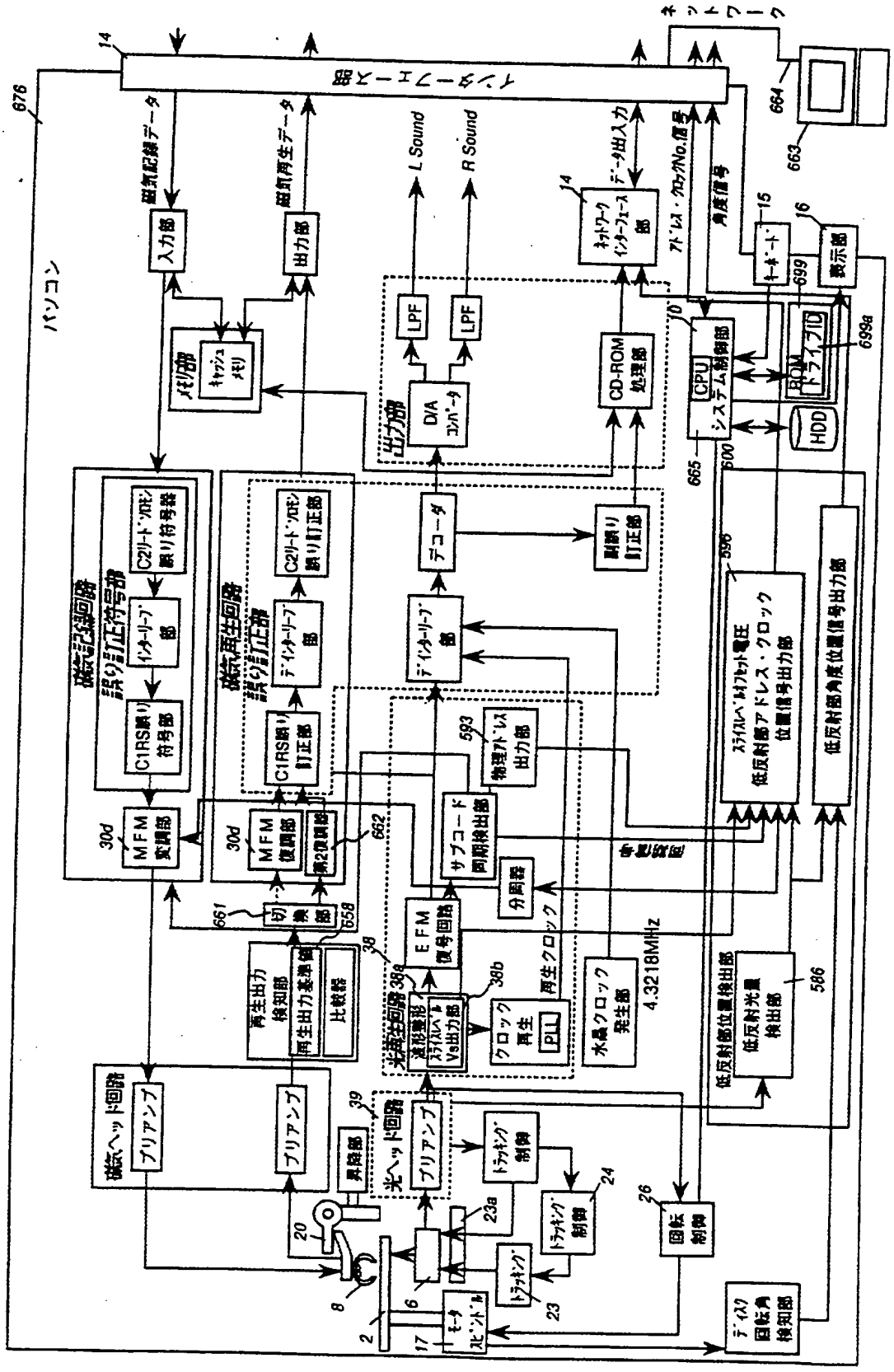
第3原盤 ▲ CLV=1.308m／sec(FZ-SJ1951AT 8)



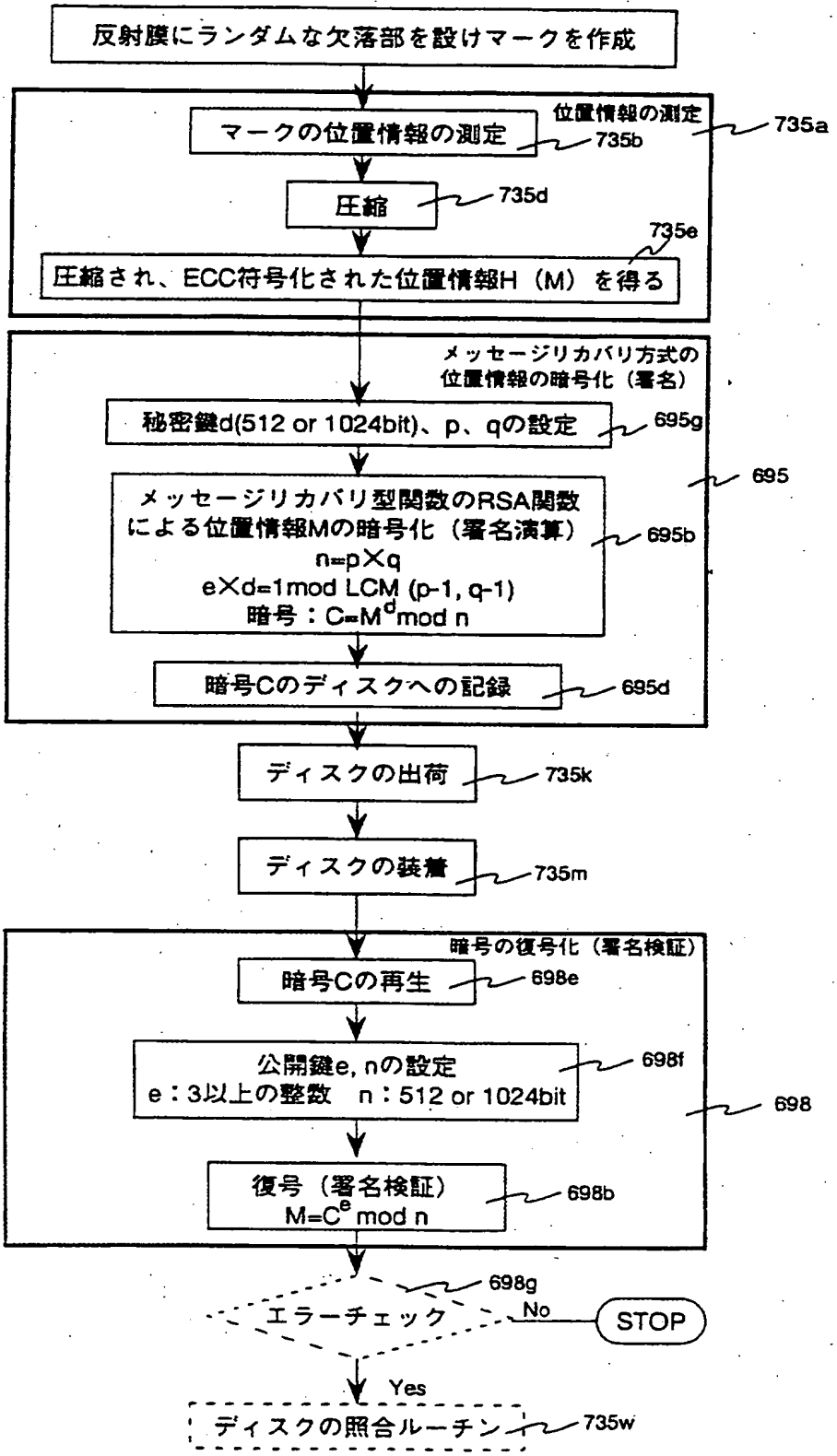
第２０図


光マークをより正確にもしくは安定して検出するための再生装置の中のプログラム
Yes
865a
暗号化された位置情報の入手
位置情報表作成ルーチン
複号or署名検証
865b
位置情報表の作成（光学マーク番号：m、ｱﾄﾞﾚｽ：nm、開始、終了ﾌﾚｰﾑSync番号、ｸﾛｯｸ番号：Tsm,TEm）
865c
865d
アドレス：ns-1を検知
回路遅延時間TDの測定ルーチン
865y
ﾌﾚｰﾑSync番号とｸﾛｯｸをｶｳﾝﾄ
回路遅延時間をROMより読み出す
865h
865i
基準無反射信号を検知？
No
Yes
回路遅延時間：TDを測定、記憶
865g
m=0
865x
m=m+1
865z
865i
アドレス：nm-1を検知
光学ﾏｰｸmのｱﾄﾞﾚｽ・ｸﾛｯｸ数検出ﾙｰﾁﾝ
865j
Frame Sync No, ｸﾛｯｸをｶｳﾝﾄ
865k
無反射信号を検知？
No
次のアドレス信号を検出？
No
Yes
Yes
開始Frame Sync No, ｸﾛｯｸ数：Tsmと終了ｸﾛｯｸ数TmEを測定
865m
海賊版ディスク検知ルーチン
回路遅延時間TDの補正
Tsm - TD = Ts'm
TEm - TD = TE'm
865n
許容誤差866：tAと合格回数の読み出し誤検出回数許容値：NA
865p
位置情報が許容範囲内にあるかを照合
tsm - tA < Ts'm < Tsm + tA
tEm - tA < TE'm < TEm + tA
865q
OK？
No
865r
Yes
照合ﾏｰｸ数=合格回数？
865s
No
Yes
誤検出回数<NA?
865t
Yes
NO
正規ディスクと判定
865u
不正ディスクと判定
865v
RUN
STOP

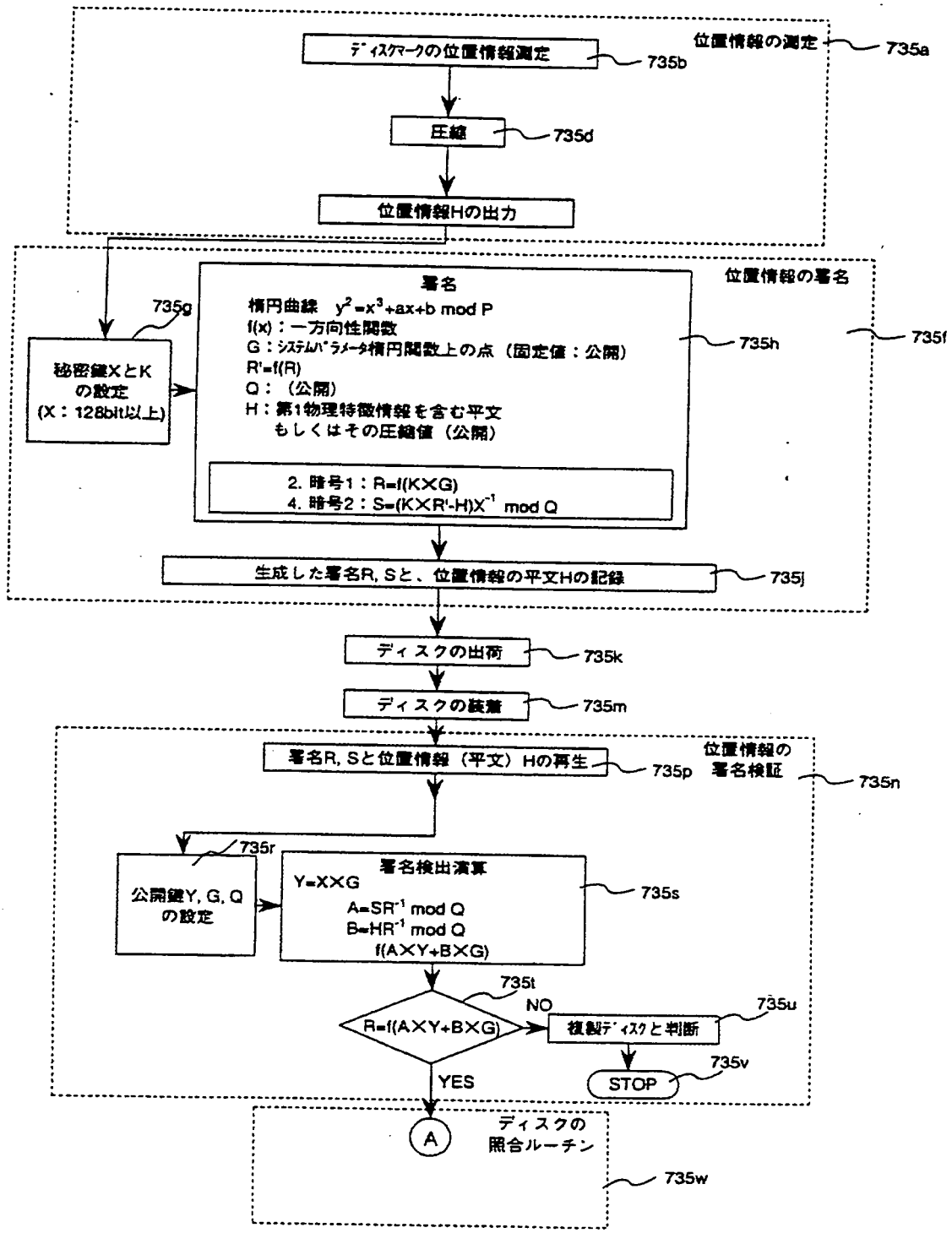
第２１図


パソコン
14
676
磁気記録データ
磁気再生データ
入力部
出力部
メモリ部
キャッシュメモリ
L Sound
R Sound
LPF
LPF
D/A コンバータ
出力部
ネットワークインターフェース部
データ出入力
アドレス・カウントNo.信号
角度信号
CD-ROM 処理部
CPU
システム制御部
ROM
ドライブ10
HDD
665
600
キーボード
15
16
表示部
699
699a
664
663
ネットワーク
磁気記録
誤り訂正符号部
C2シンドローム
誤り符号器
インターリーブ部
C1RS誤り符号部
MFM 変調部
30d
磁気再生回路
誤り訂正部
C2シンドローム
誤り訂正部
デインターリーブ部
C1RS誤り訂正部
MFM 復調部
第2復調部
662
30d
デコーダ
訂正部
デインターリーブ部
593
物理アドレス出力部
サブコード同期検出部
分周器
切換部
661
658
38
EFM 復号回路
38a
38b
光再生回路
波形整形
スライスレベル
Vs出力部
クロック再生
PLL
再生クロック
水晶クロック発生部
4.3218MHz
再生出力検知部
再生出力基準値
比較器
磁気ヘッド回路
プリアンプ
昇降部
39
光ヘッド回路
プリアンプ
トラッキング制御
トラッキング制御
トラッキング
回転制御
26
24
23a
23
20
8
6
2
17
モータ
スピンドル
ディスク回転角検知部
スライスレベル電圧
低反射部アドレス・クロック
位置信号出力部
596
低反射部位置角度位置信号出力部
低反射部位置検出部
低反射光量検出部
586
各記録面

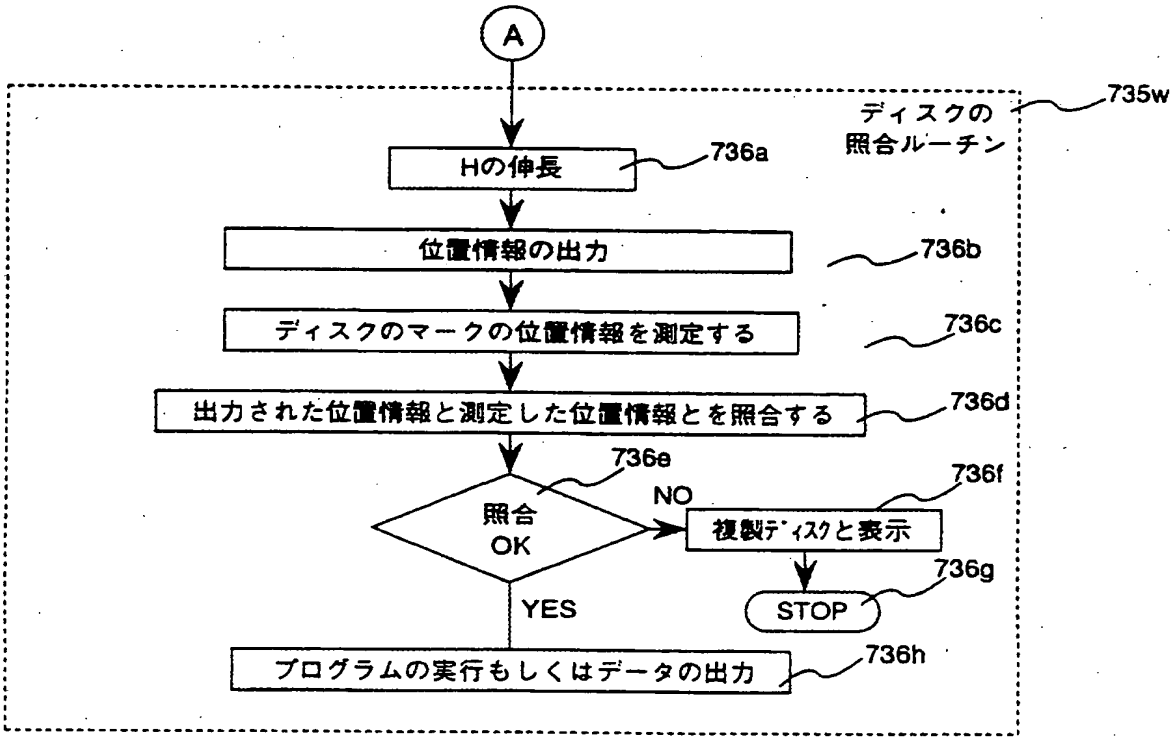
第２２図


反射膜にランダムな欠落部を設けマークを作成
位置情報の測定
735a
マークの位置情報の測定
735b
圧縮
735d
735e
圧縮され、ECC符号化された位置情報H（M）を得る
メッセージリカバリ方式の
位置情報の暗号化（署名）
秘密鍵d(512 or 1024bit)、p、qの設定
695g
695
メッセージリカバリ型関数のRSA関数
による位置情報Mの暗号化（署名演算）
695b
n=p×q
e×d=1mod LCM (p-1, q-1)
暗号：C=M^d mod n
暗号Cのディスクへの記録
695d
ディスクの出荷
735k
ディスクの装着
735m
暗号の復号化（署名検証）
暗号Cの再生
698e
公開鍵e, nの設定
e：3以上の整数　n：512 or 1024bit
698f
698
復号（署名検証）
M=C^e mod n
698b
698g
エラーチェック
No
STOP
Yes
ディスクの照合ルーチン
735w

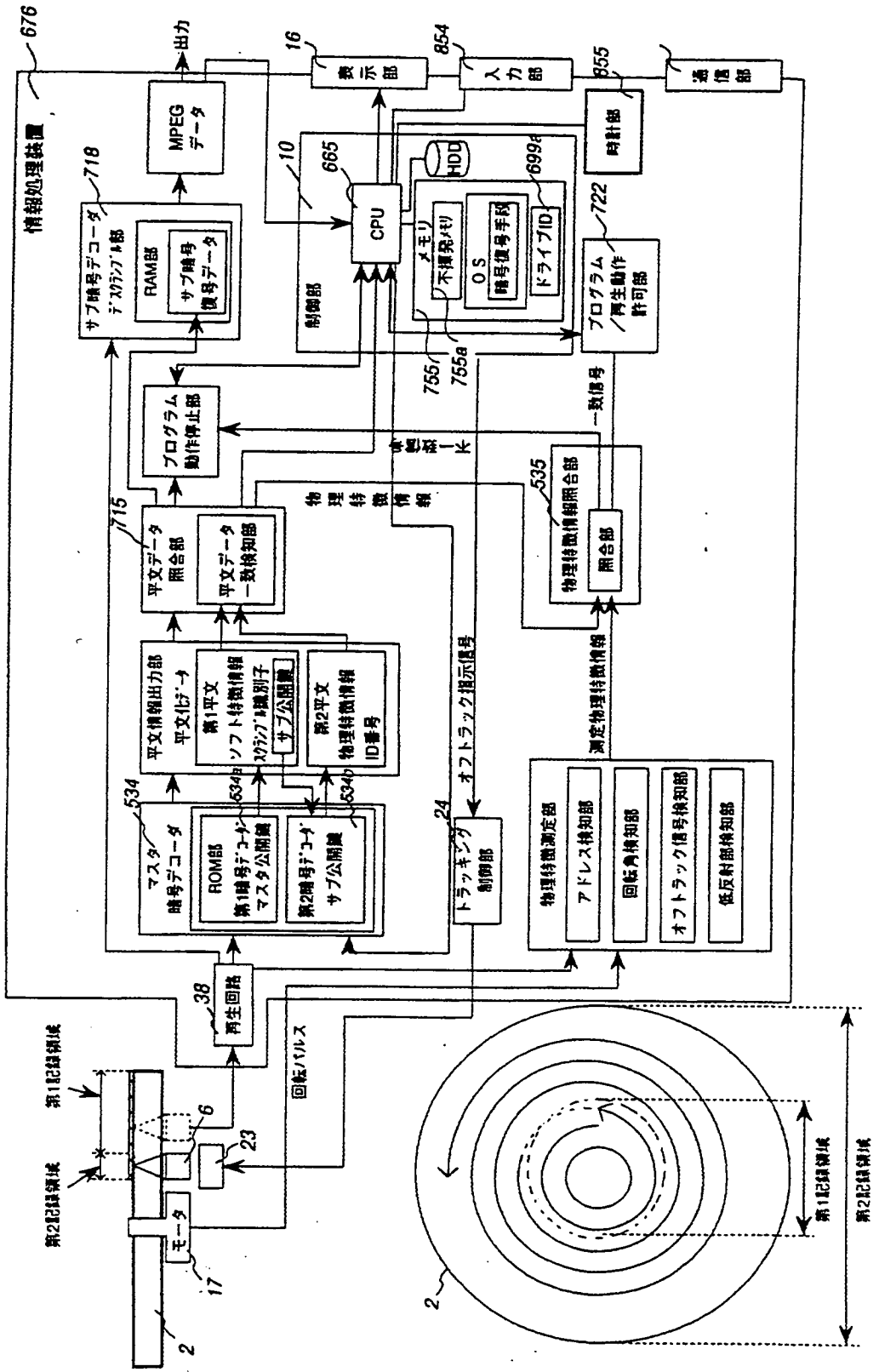
第２３図

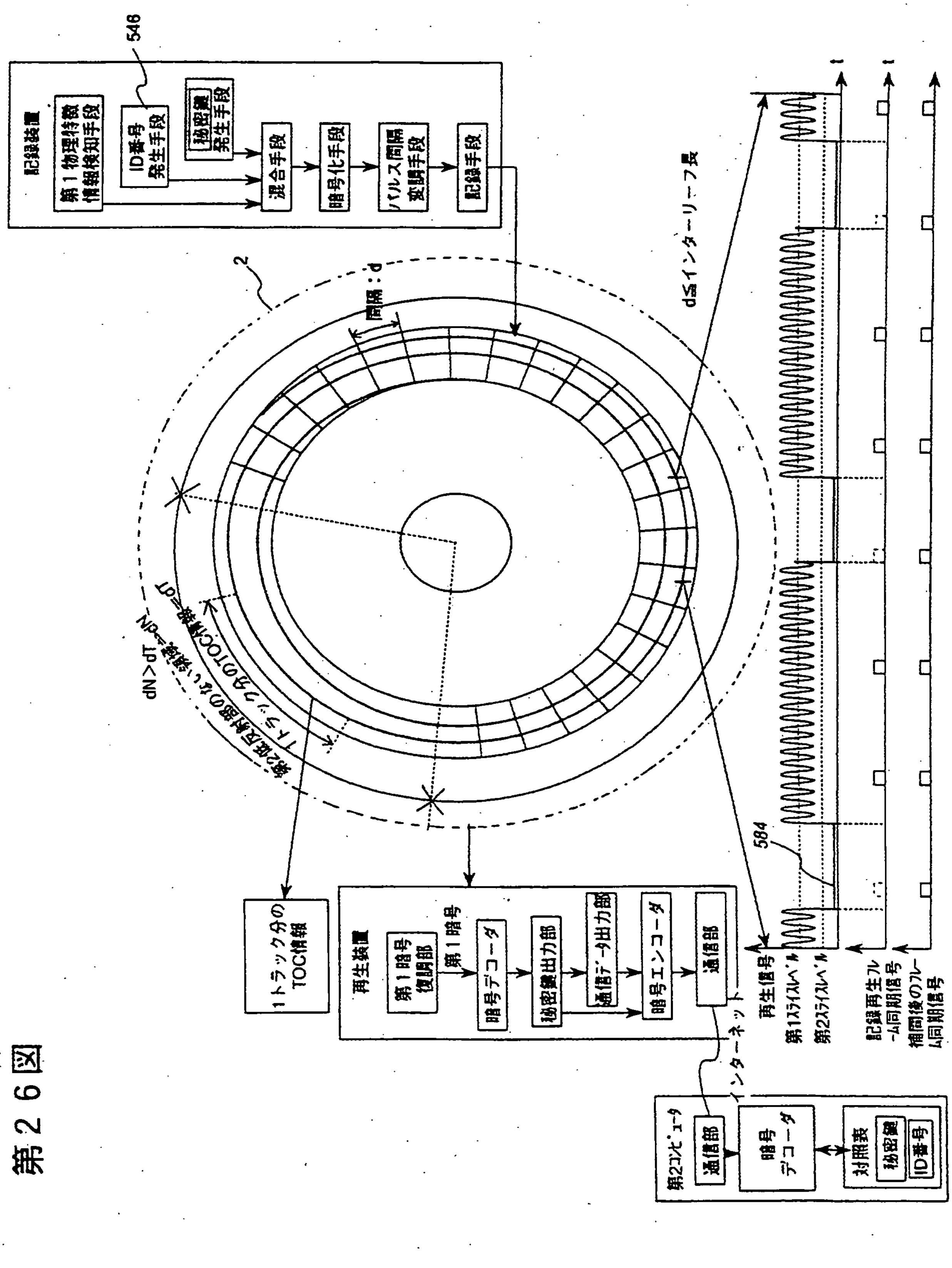

位置情報の測定
735a
ﾃﾞｨｽｸﾏｰｸの位置情報測定
735b
圧縮
735d
位置情報Hの出力
位置情報の署名
735f
735g
秘密鍵XとK
の設定
(X：128bit以上)
署名
楕円曲線 $y^2=x^3+ax+b \bmod P$
f(x)：一方向性関数
G：ｼｽﾃﾑﾊﾟﾗﾒｰﾀ楕円関数上の点（固定値：公開）
R'=f(R)
Q：（公開）
H：第1物理特徴情報を含む平文
もしくはその圧縮値（公開）
735h
2. 暗号1：R=f(K×G)
4. 暗号2：$S=(K\times R'-H)X^{-1} \bmod Q$
生成した署名R, Sと、位置情報の平文Hの記録
735j
ディスクの出荷
735k
ディスクの装着
735m
位置情報の
署名検証
735n
署名R, Sと位置情報（平文）Hの再生
735p
735r
公開鍵Y, G, Q
の設定
署名検出演算
Y=X×G
$A=SR^{-1} \bmod Q$
$B=HR^{-1} \bmod Q$
f(A×Y+B×G)
735s
735t
R=f(A×Y+B×G)
NO
複製ﾃﾞｨｽｸと判断
735u
735v
STOP
YES
A
ディスクの
照合ルーチン
735w

第２４図


A
ディスクの
照合ルーチン
735w
Hの伸長
736a
位置情報の出力
736b
ディスクのマークの位置情報を測定する
736c
出力された位置情報と測定した位置情報とを照合する
736d
736e
照合
OK
NO
736f
複製ディスクと表示
736g
STOP
YES
プログラムの実行もしくはデータの出力
736h

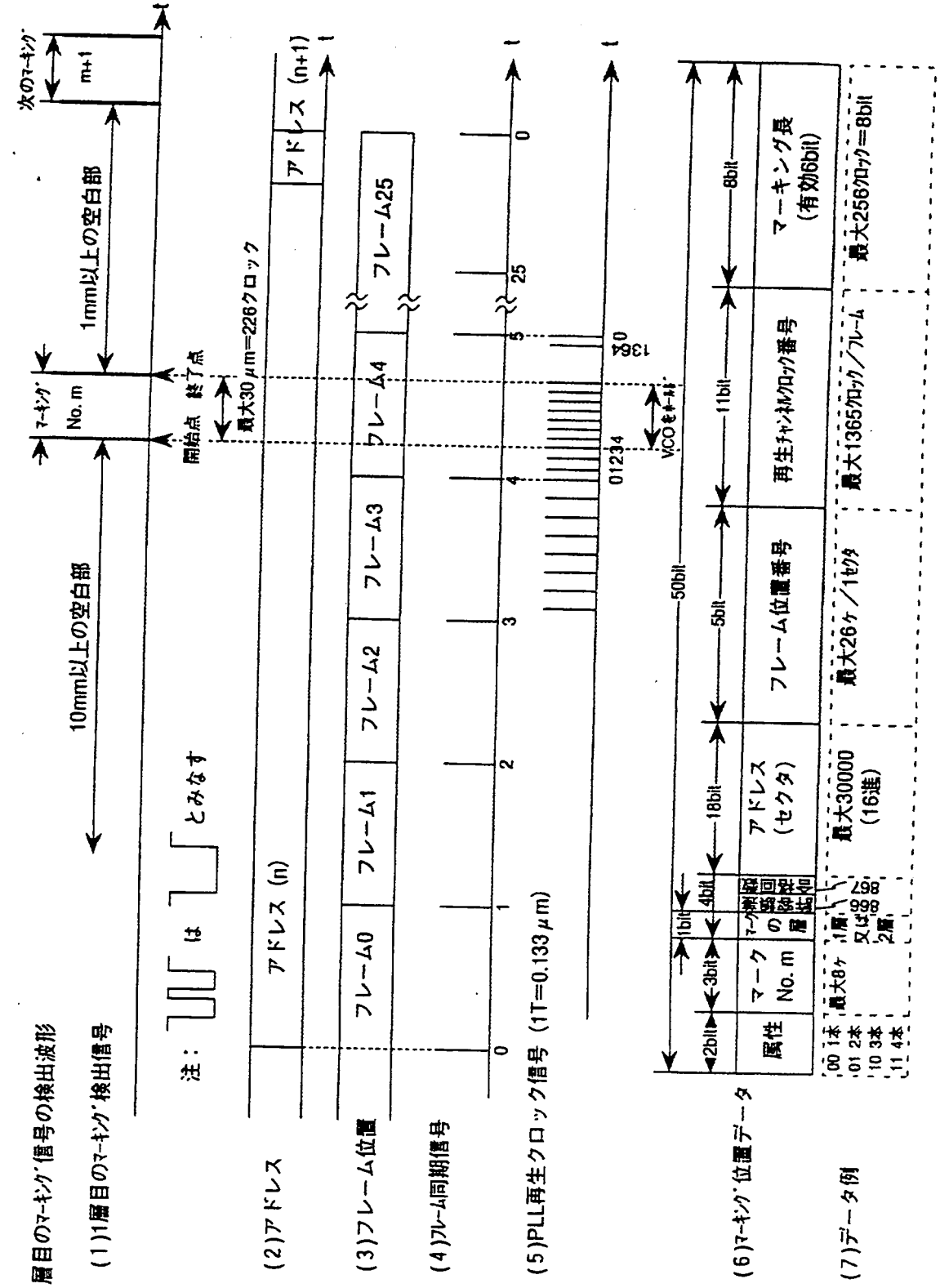
第25図


676
情報処理装置
出力
MPEGデータ
718
サブ暗号デコーダ
RAM部
サブ暗号復号データ
16
表示部
854
入力部
855
通信部
10
制御部
665
CPU
HDD
699a
メモリ
不揮発メモリ
OS
暗号復号手段
ドライブID
時計部
722
プログラム再生動作許可部
755
755a
プログラム動作停止部
715
平文データ照合部
平文データ一致検知部
平文情報出力部
平文化データ
第1平文ソフト特徴情報
ソフト識別子
サブ公開鍵
第2平文物理特徴情報
ID番号
534
マスター暗号デコーダ
ROM部
第1暗号データ
マスター公開鍵
第2暗号データ
サブ公開鍵
534a
534b
24
トラッキング制御部
オフトラック指示信号
535
物理特徴情報照合部
照合部
物理特徴情報
一致信号
測定物理特徴情報
物理特徴測定部
アドレス検知部
回転角検知部
オフトラック信号検知部
低反射部検知部
38
再生回路
回転パルス
第1記録領域
第2記録領域
6
23
モータ
17
2

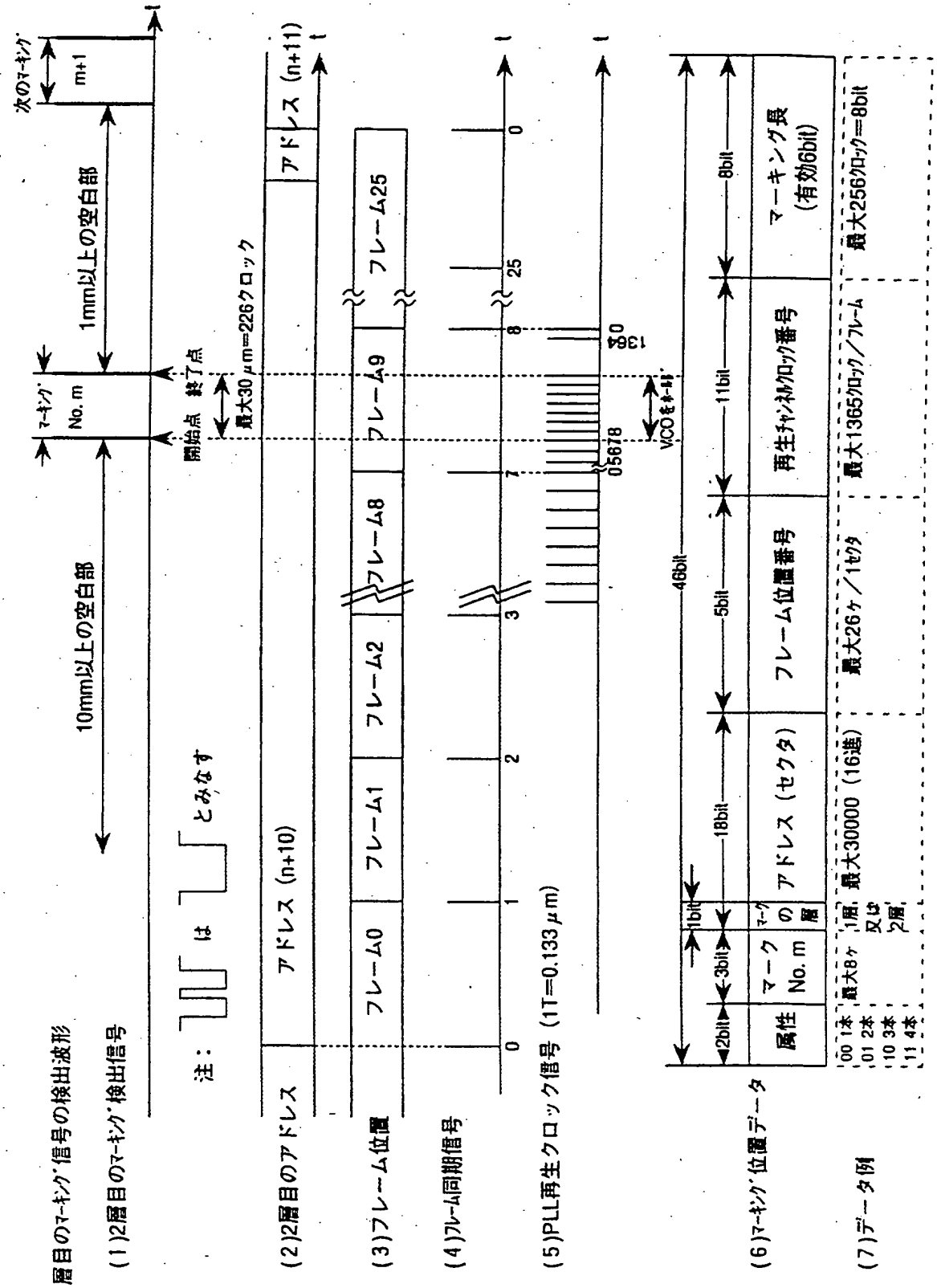

記録装置
第１物理特徴
情報検知手段
ID番号
発生手段
546
秘密鍵
発生手段
混合手段
暗号化手段
パルス間隔
変調手段
記録手段
2
間隔：d
d≦インターリーブ長
dN＞dT
第2低反射部のない領域＝dN
1トラック分のTOC領域＝dT
1トラック分の
TOC情報
再生装置
第１暗号
復調部
第１暗号
暗号デコーダ
秘密鍵出力部
通信データ出力部
暗号エンコーダ
通信部
インターネット
584
再生信号
第1スライスレベル
第2スライスレベル
記録再生フレーム同期信号
補間後のフレーム同期信号
第2コンピュータ
通信部
暗号
デコーダ
対照表
秘密鍵
ID番号

第２６図

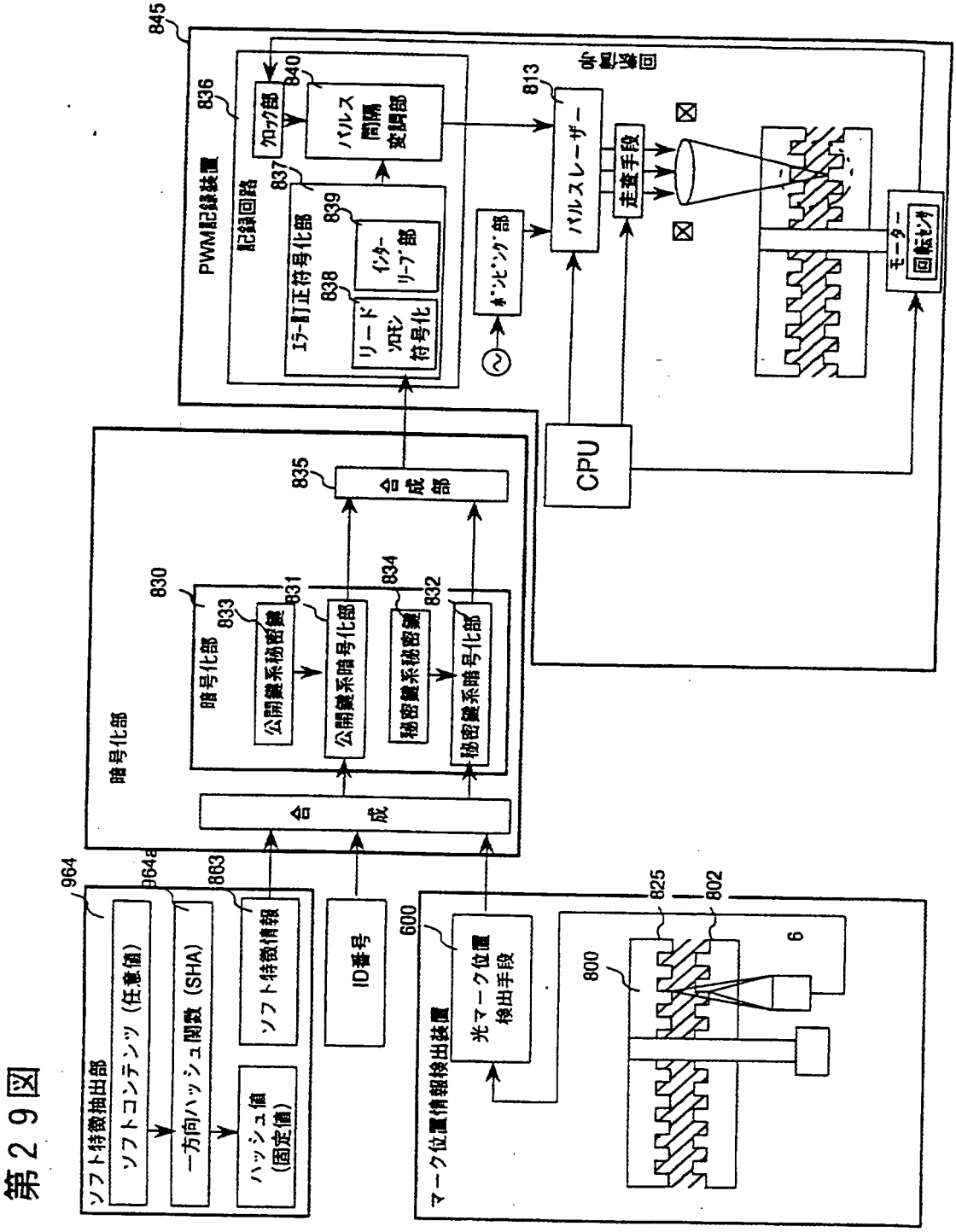
第２７図


1層目のマーキング信号の検出波形
(1)1層目のマーキング検出信号
マーキング No. m
1mm以上の空白部
次のマーキング m+1
10mm以上の空白部
開始点 終了点
最大30μm=226クロック
注：「」は「」とみなす
(2)アドレス
アドレス (n)
アドレス (n+1)
(3)フレーム位置
フレーム0
フレーム1
フレーム2
フレーム3
フレーム4
フレーム25
(4)フレーム同期信号
0 1 2 3 4 5 25 0
(5)PLL再生クロック信号 (1T=0.133μm)
01234
138
VCOモード
(6)マーキング位置データ
1bit
2bit
3bit
4bit
18bit
5bit
50bit
11bit
8bit
属性
マーク No. m
マークの検出回数
アドレス (セクタ)
フレーム位置番号
再生チャンネルクロック番号
マーキング長 (有効6bit)
(7)データ例
00 1本
01 2本
10 3本
11 4本
最大8ヶ
1層、又は2層、
最大30000 (16進)
最大26ヶ／1セクタ
最大1365クロック／フレーム
最大256クロック=8bit

第２８図


2層目のマーキング信号の検出波形
(1)2層目のマーキング検出信号
次のマーキング
m+1
1mm以上の空白部
マーキング
No. m
10mm以上の空白部
開始点 終了点
最大30μm=226クロック
注：
は
とみなす
(2)2層目のアドレス
アドレス (n+10)
アドレス (n+11)
(3)フレーム位置
フレーム0
フレーム1
フレーム2
フレーム8
フレーム9
フレーム25
(4)フレーム同期信号
0
1
2
3
7
8
25
(5)PLL再生クロック信号 (1T=0.133μm)
05678
VCOモード
(6)マーキング位置データ
46bit
2bit
3bit
1bit
18bit
5bit
11bit
8bit
属性
マークNo. m
マークの層
アドレス (セクタ)
フレーム位置番号
再生チャンネルクロック番号
マーキング長 (有効6bit)
(7)データ例
00 1本
01 2本
10 3本
11 4本
最大8ヶ所
1層、最大30000 (16進)
又は
2層
最大26ヶ所／セクタ
最大1365クロック／フレーム
最大256クロック=8bit

第２９図


845
836
PWM記録装置
記録回路
840
カット部
パルス間隔変調部
837
839
エラー訂正符号化部
インターリーブ部
838
リードソロモン符号化
813
パルスレーザー
走査手段
ポンピング部
回転制御部
モーター
回転センサ
CPU
835
合成部
830
暗号化部
833
公開鍵系秘密鍵
831
公開鍵系暗号化部
834
秘密鍵系秘密鍵
832
秘密鍵系暗号化部
合成
964
964a
863
ソフト特徴抽出部
ソフトコンテンツ（任意値）
一方向ハッシュ関数（SHA）
ハッシュ値（固定値）
ソフト特徴情報
ID番号
600
マーク位置情報検出装置
光マーク位置検出手段
825
802
800
6

第３０図

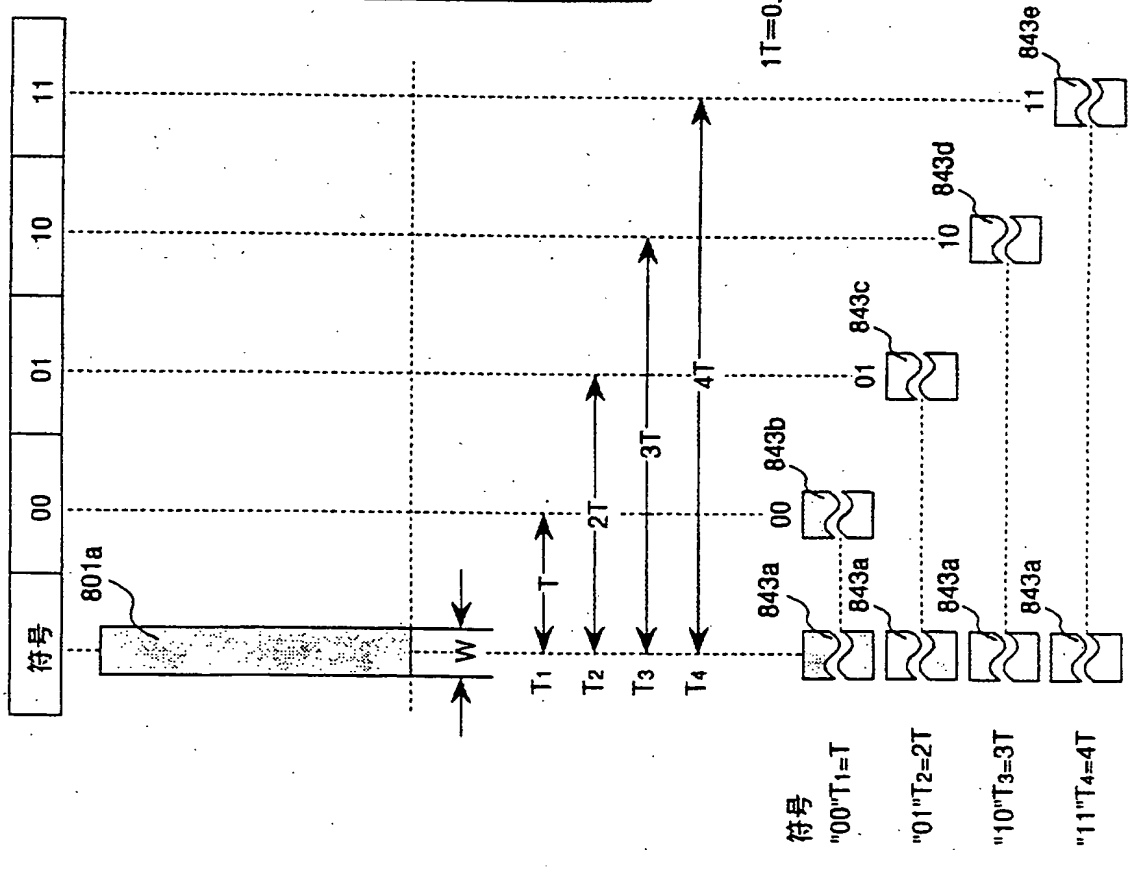
バーコードの線巾と記録密度の関係

線巾	周期	記録密度	最大記録容量	1Kbitの長さ
W（μm）	T（μm）	μm／bit	1周分	mm
1μm	2μm	2.55μm	56Kbit	2.5mm
3μm	6μm	7.5μm	28.2Kbit	5mm
5μm	10μm	12.5μm	11.2Kbit	12.5mm
10μm	20μm	25μm	5.6Kbit	25mm
20μm	40μm	50μm	2.82Kbit	50mm

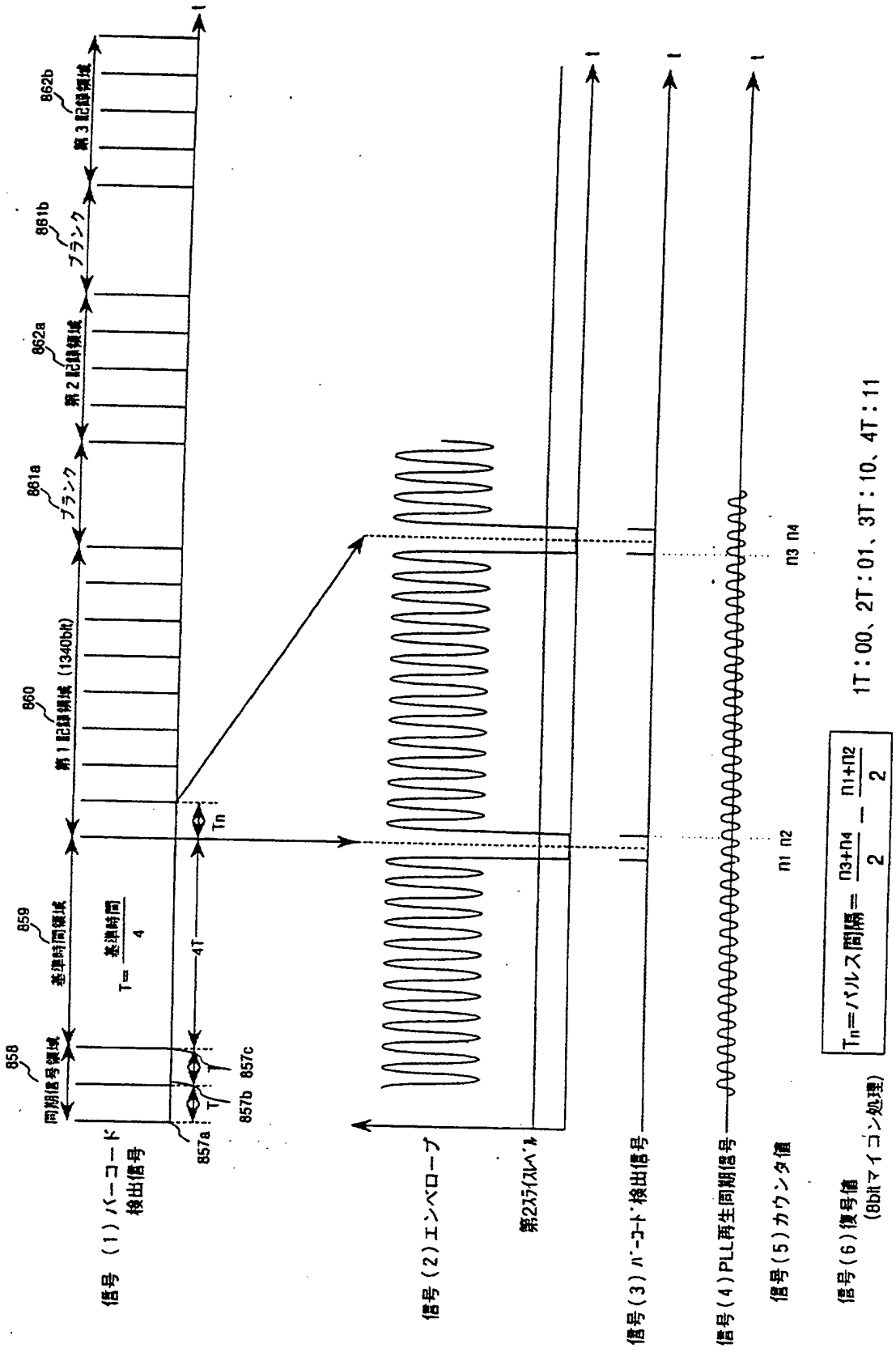
842

4値PWM記録の場合のパルス間隔別の符号

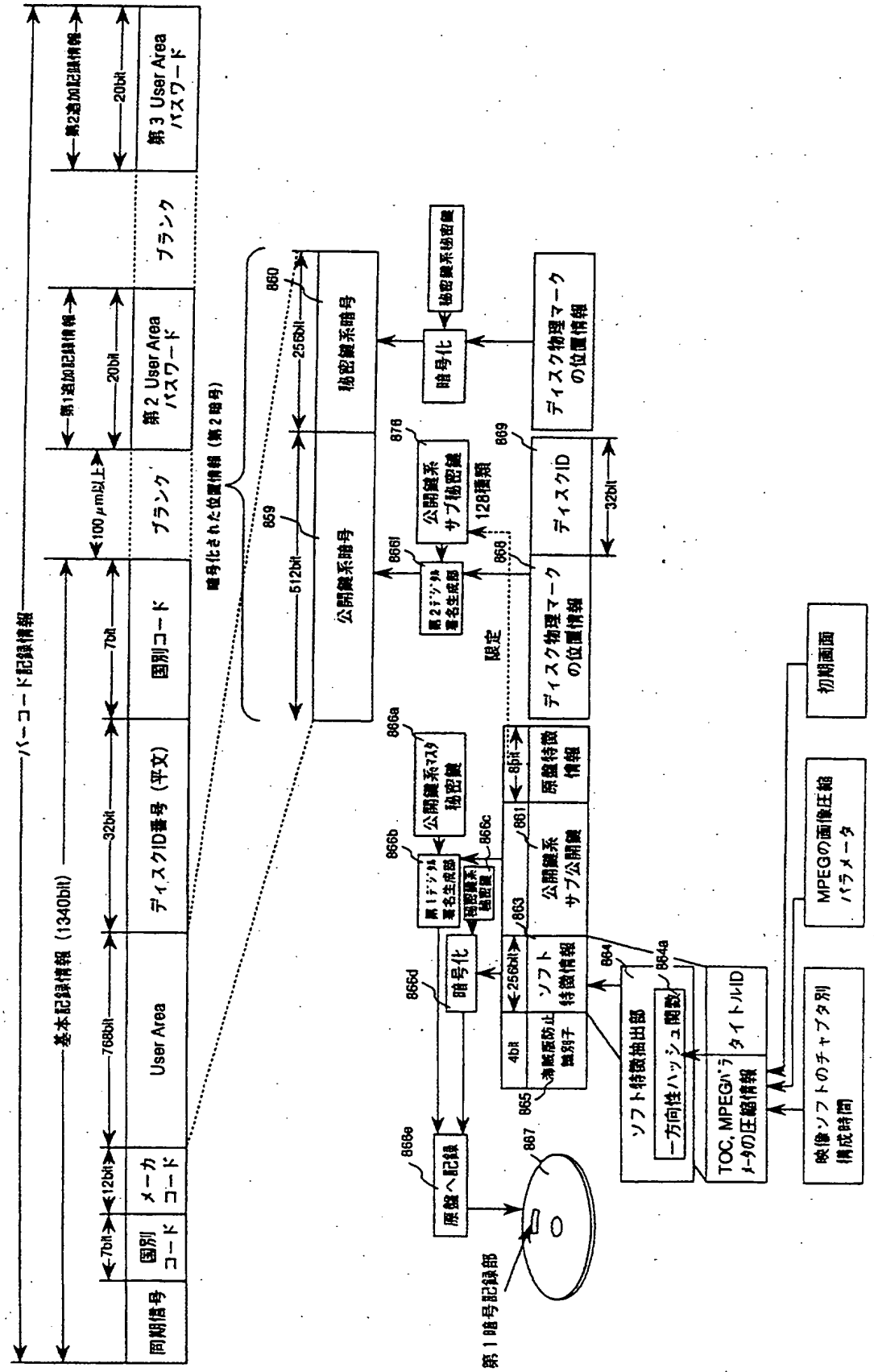
符号	00	01	10	11



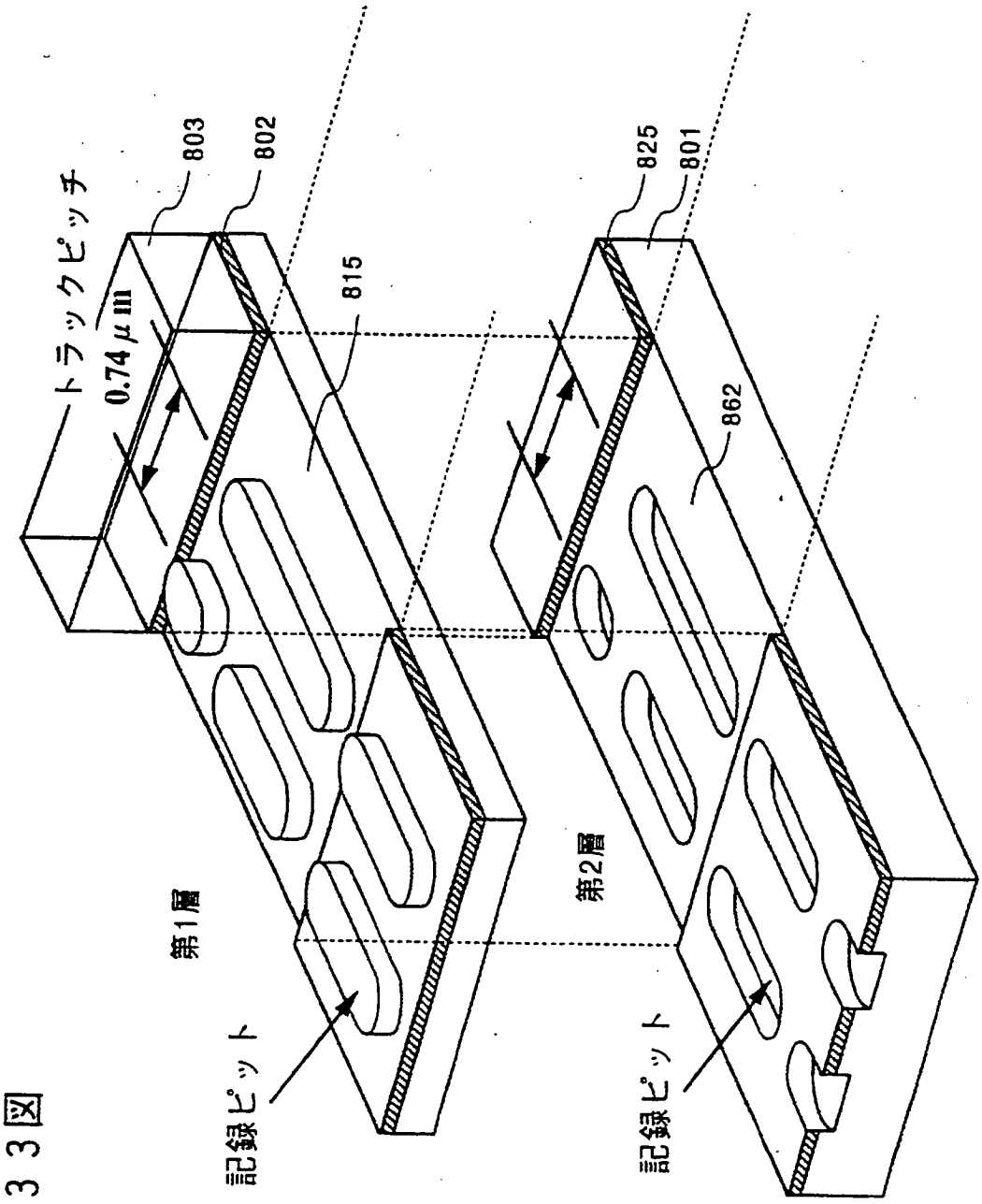
第３１図


信号（１）バーコード検出信号
信号（２）エンベロープ
信号（３）バーコード検出信号
信号（４）PLL再生同期信号
信号（５）カウンタ値
信号（６）復号値
(8bitマイコン処理)
858 同期信号領域
859 基準時間領域
860 第１記録領域（1340bit）
861a ブランク
862a 第２記録領域
861b ブランク
862b 第３記録領域
T= 基準時間 / 4
4T
Tn
857a 857b 857c
第2スライスレベル
n1 n2
n3 n4
Tn=パルス間隔= (n3+n4)/2 − (n1+n2)/2
1T：00、2T：01、3T：10、4T：11

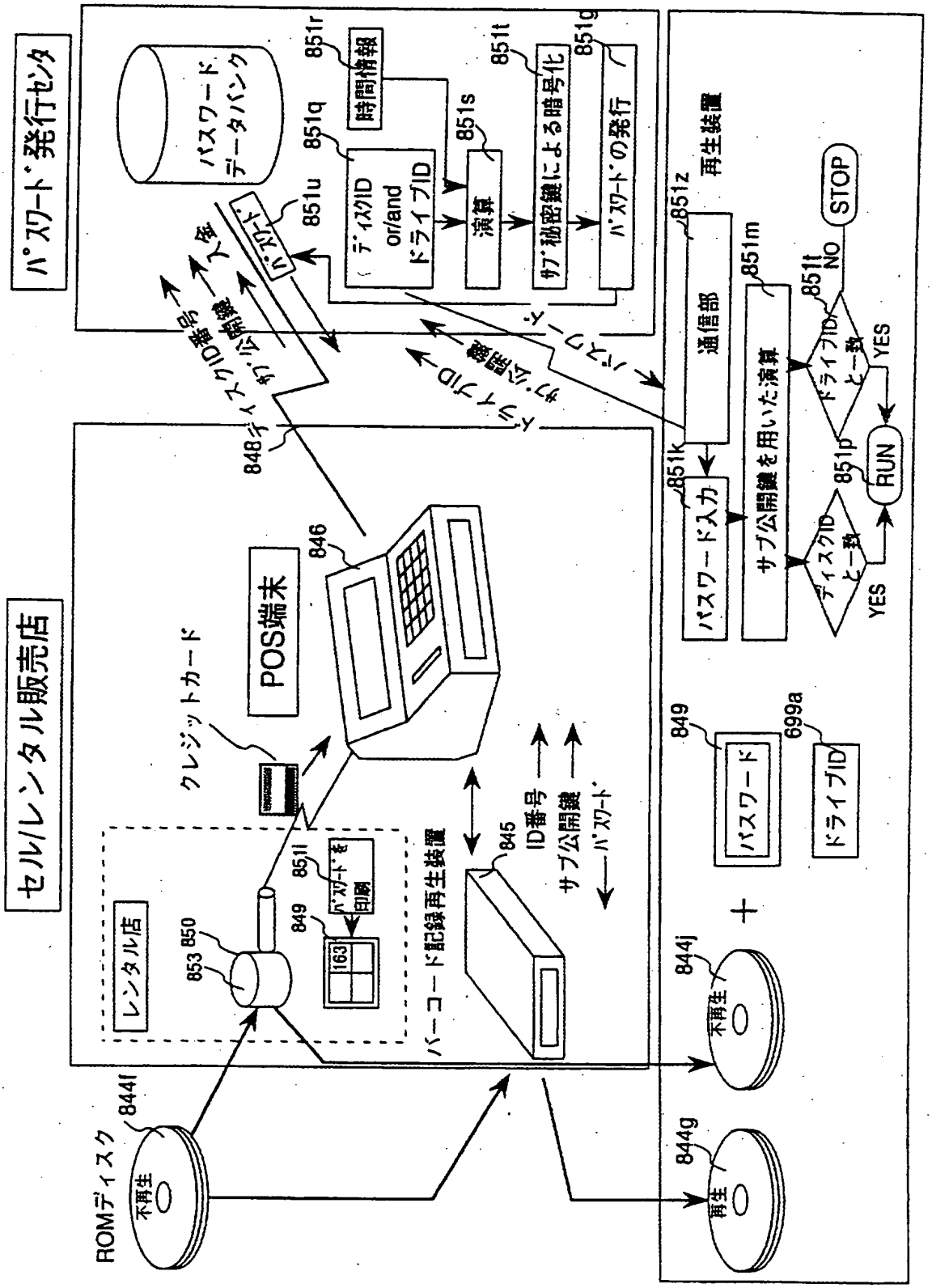
第３２図


バーコード記録情報
基本記録情報（1340bit）
同期情号
国別コード
メーカコード
User Area
ディスクID番号（平文）
国別コード
ブランク
第2 User Area パスワード
ブランク
第3 User Area パスワード
7bit
12bit
768bit
32bit
7bit
100μm以上
20bit
第1追加記録情報
20bit
第2追加記録情報
暗号化された位置情報（第2暗号）
公開鍵系暗号
秘密鍵系暗号
512bit
256bit
860
859
暗号化
秘密鍵系秘密鍵
ディスク物理マークの位置情報
878
公開鍵系サブ秘密鍵
128種類
669
ディスクID
32bit
第2デジタル署名生成部
866l
868
限定
ディスク物理マークの位置情報
866a
公開鍵系マスタ秘密鍵
第1デジタル署名生成部
866b
秘密鍵
866c
公開鍵系サブ公開鍵
861
85bit
原盤特徴情報
863
256bit
ソフト特徴情報
4bit
海賊版防止識別子
865
暗号化
866d
原盤へ記録
866e
第1暗号記録部
867
ソフト特徴抽出部
864
864a
一方向性ハッシュ関数
タイトルID
TOC, MPEGパラメータの圧縮情報
映像ソフトのチャプタ別構成時間
MPEGの画像圧縮パラメータ
初期画面

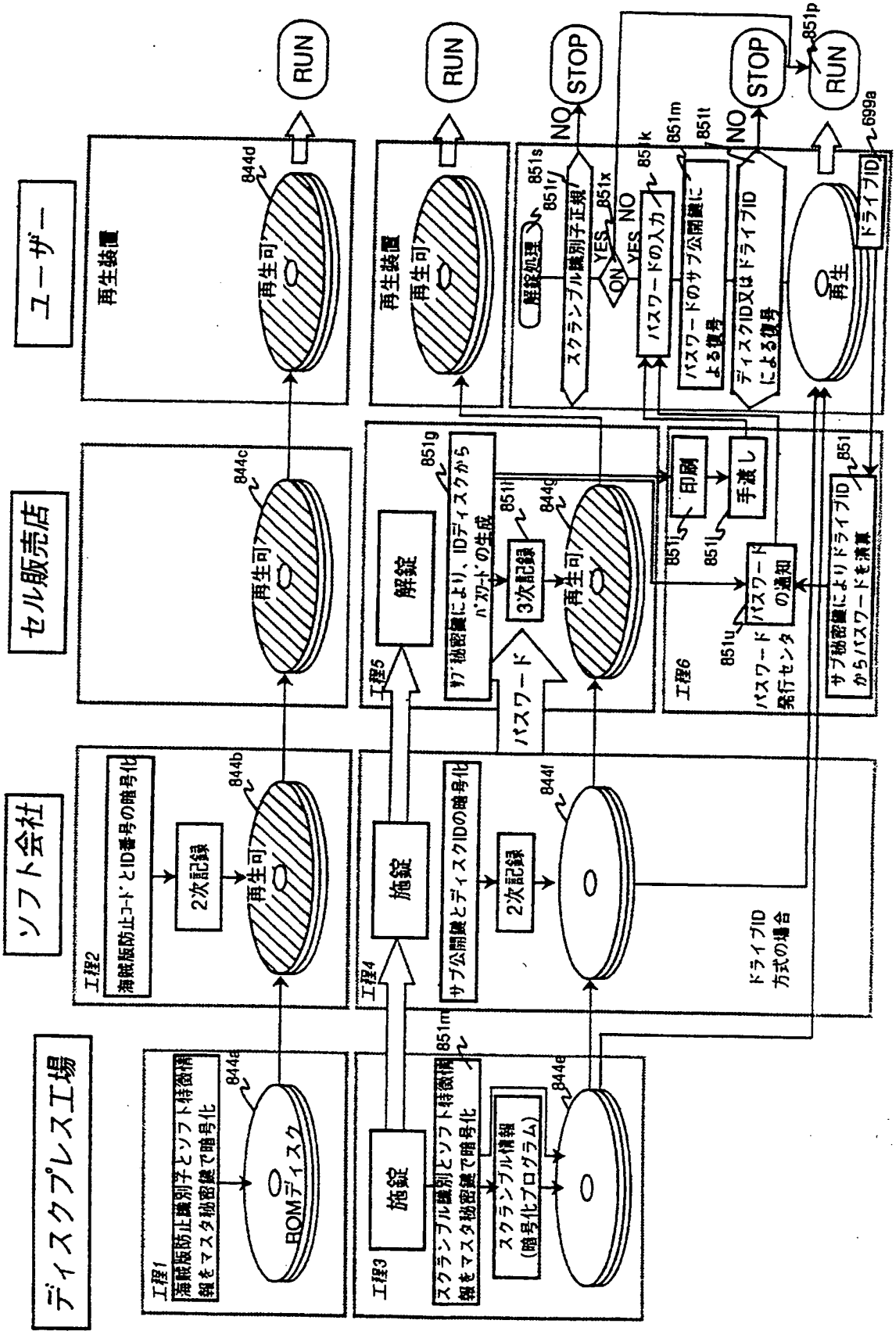
第３３図



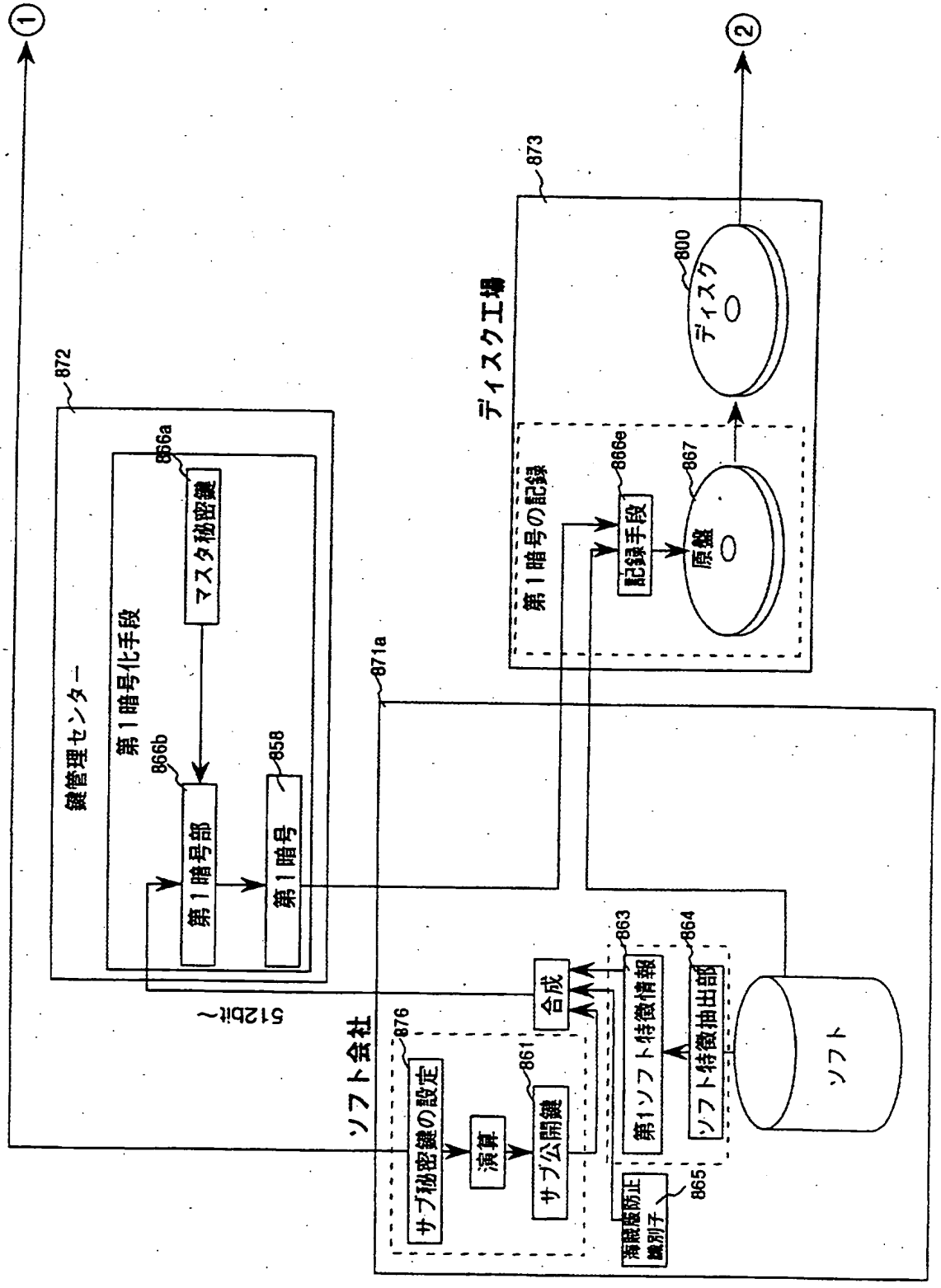
第３４図

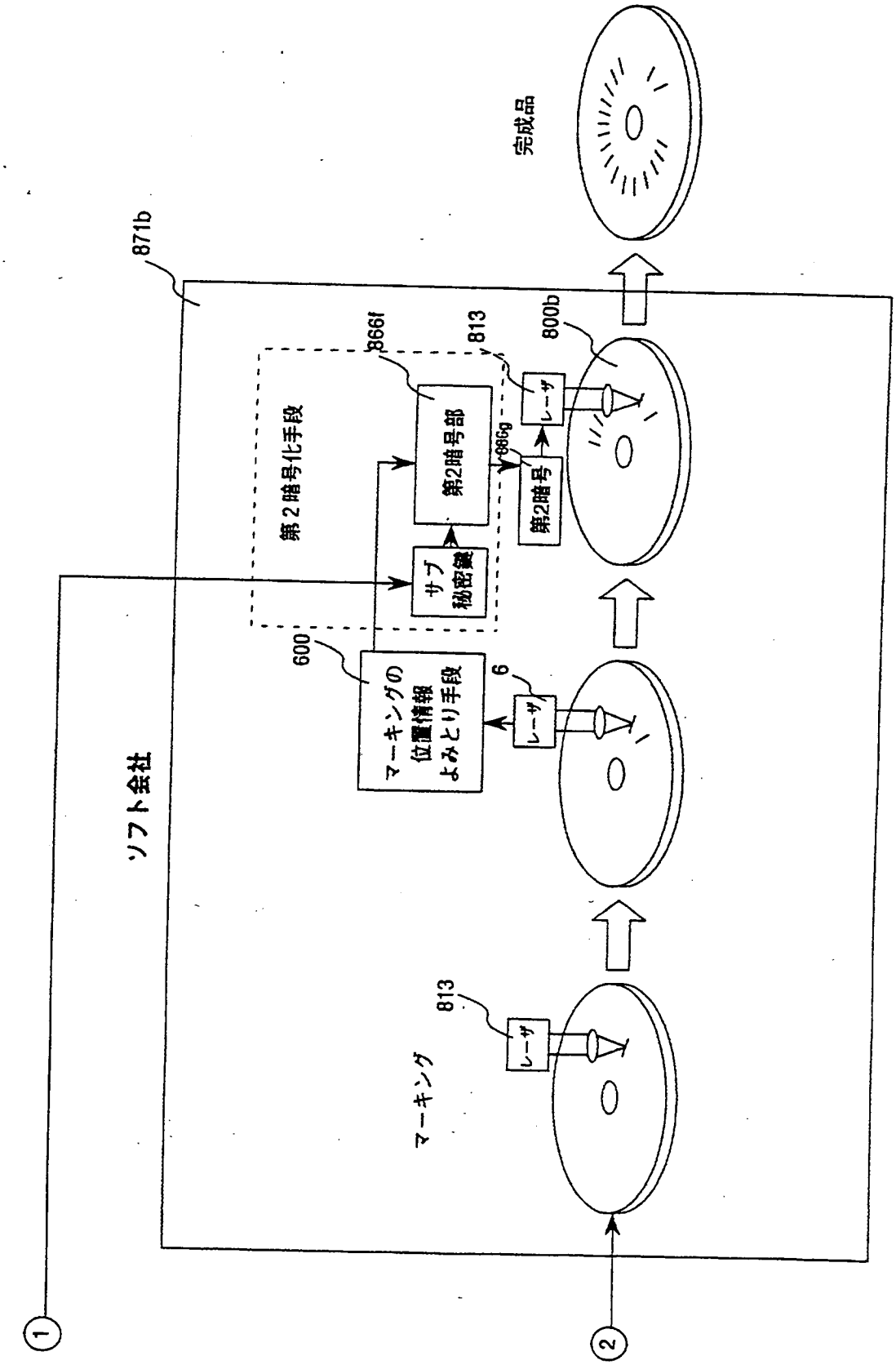

パスワード発行センタ
パスワードデータバンク
851r
時間情報
851q
ディスクID or/and ドライブID
851s
演算
851t
サブ秘密鍵による暗号化
851g
パスワードの発行
851u
パスワード
848
ディスクID番号
サブ公開鍵
ユーザID
パスワード
セル/レンタル販売店
POS端末
846
クレジットカード
レンタル店
853
850
849
163
851l
パスワードを印刷
バーコード記録再生装置
845
ID番号
サブ公開鍵
パスワード
ROMディスク
8441
不再生
844g
再生
844j
不再生
849
パスワード
699a
ドライブID
+
再生装置
851z
通信部
851k
パスワード入力
851m
サブ公開鍵を用いた演算
851p
ディスクID と一致
YES
851l
ドライブID と一致
NO
YES
RUN
STOP

第３５図


ディスクプレス工場
ソフト会社
セル販売店
ユーザー
工程1
海賊版防止識別子とソフト特徴情報をマスタ秘密鍵で暗号化
ROMディスク
844a
工程2
海賊版防止コードとID番号の暗号化
2次記録
再生可
844b
工程3
スクランブル識別とソフト特徴情報をマスタ秘密鍵で暗号化
851m
施錠
スクランブル情報（暗号化プログラム）
844e
工程4
施錠
サブ公開鍵とディスクIDの暗号化
2次記録
844f
工程5
解錠
851g
サブ秘密鍵により、IDディスクからパスワードの生成
3次記録
851h
844g
再生可
パスワード
工程6
印刷
手渡し
851i
851j
パスワード発行センタ
パスワードの通知
851u
サブ秘密鍵によりドライブIDからパスワードを精算
851
ドライブID方式の場合
再生可
844c
再生装置
再生可
844d
RUN
RUN
解錠処理
851s
スクランブル識別子正規
851r
YES
ON
NO
851x
パスワードの入力
851k
YES
NO
851m
パスワードのサブ公開鍵による復号
851l
ディスクID又はドライブIDによる復号
NO
STOP
STOP
851p
再生
ドライブID
699a
RUN

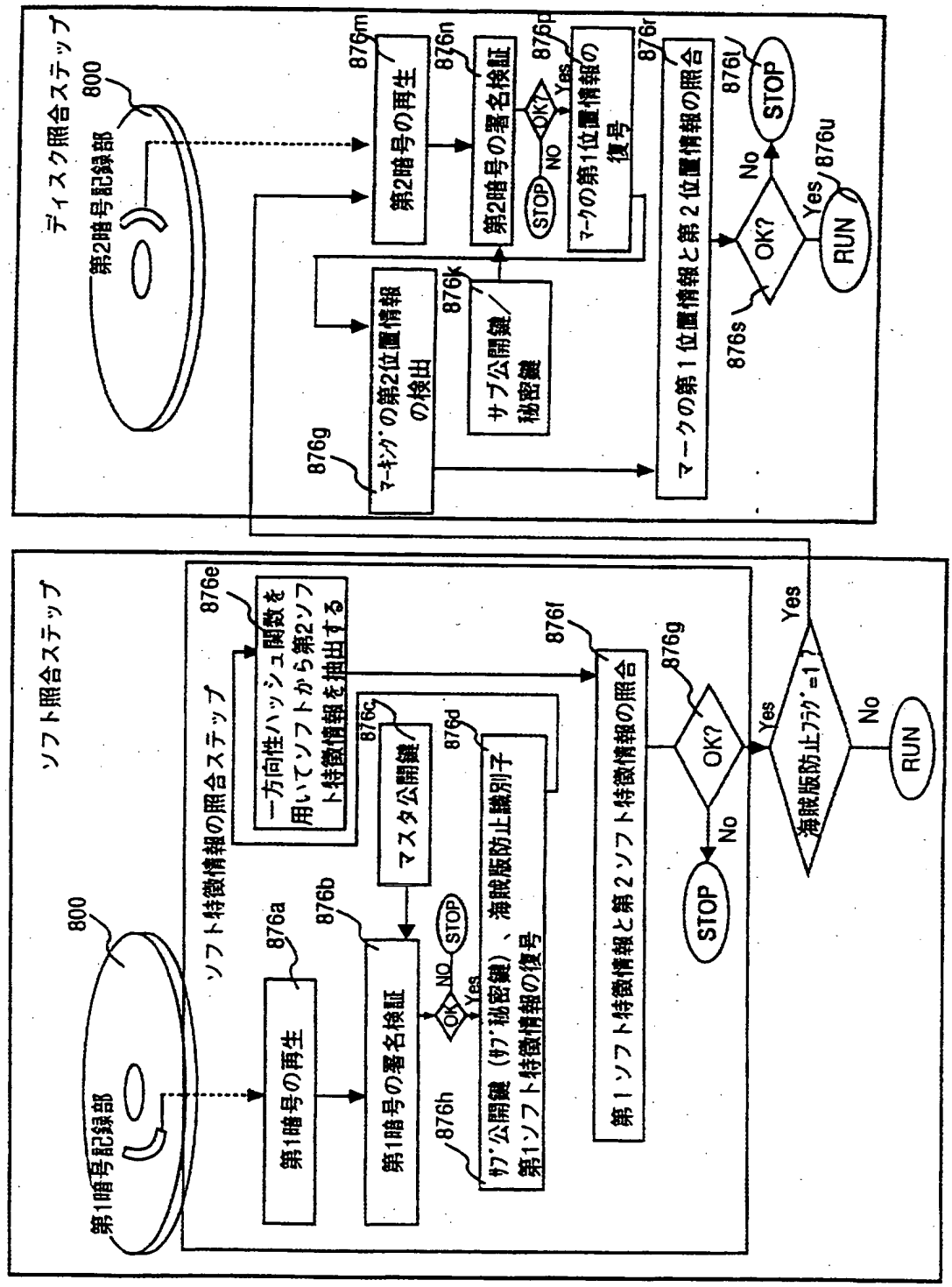
第３６図


①
②
872
鍵管理センター
第１暗号化手段
866a
マスタ秘密鍵
866b
第１暗号部
858
第１暗号
512bit
871a
ディスク工場
873
第１暗号の記録
866e
記録手段
867
原盤
800
ディスク
ソフト会社
876
サブ秘密鍵の設定
演算
861
サブ公開鍵
合成
863
第1ソフト特徴情報
864
ソフト特徴抽出部
865
海賊版防止識別子
ソフト

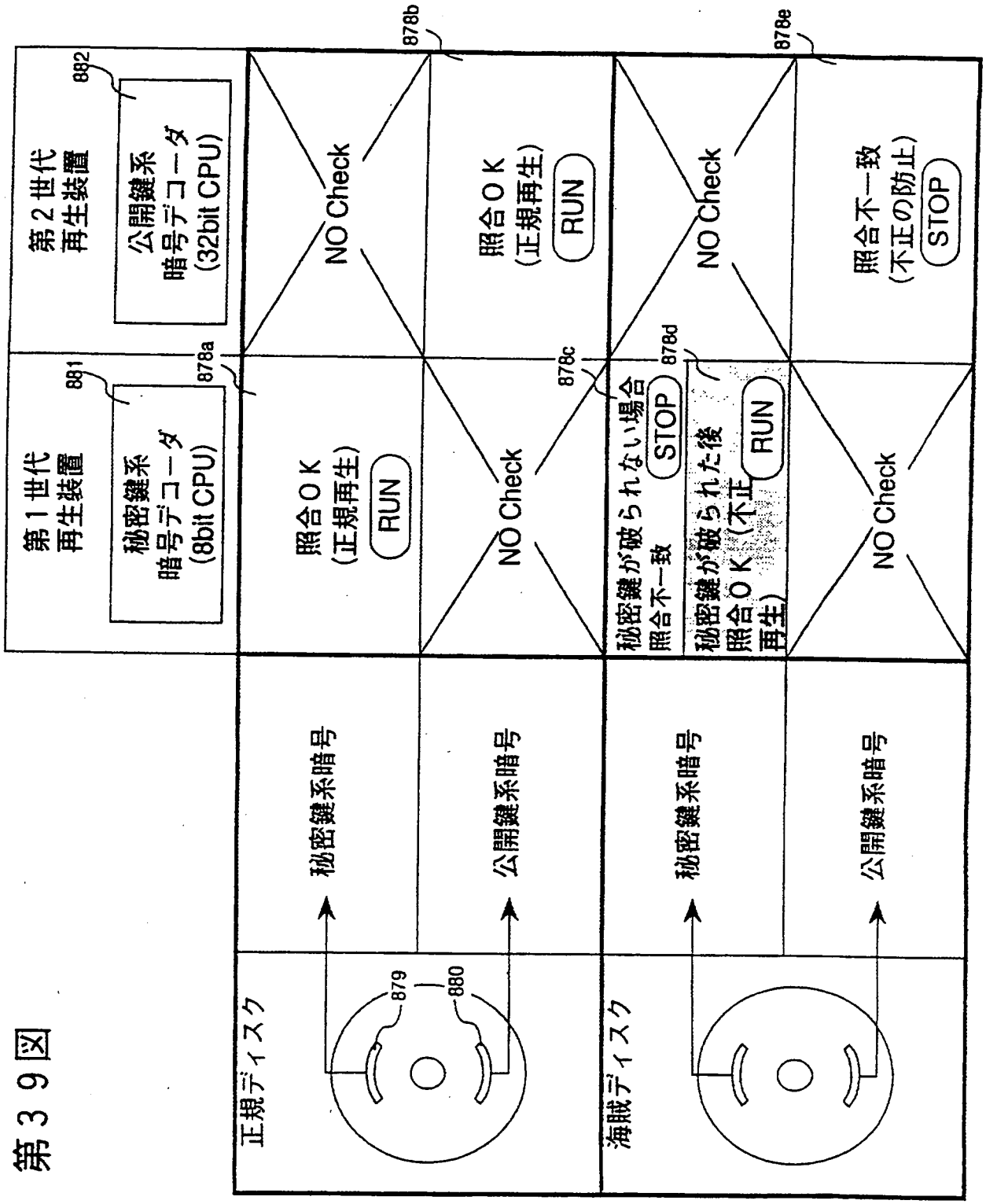

完成品
871b
800b
813
866f
第2暗号部
レーザ
886g
第2暗号
第２暗号化手段
サブ秘密鍵
600
マーキングの位置情報よみとり手段
6
レーザ
ソフト会社
813
レーザ
マーキング
①
②

第３７図

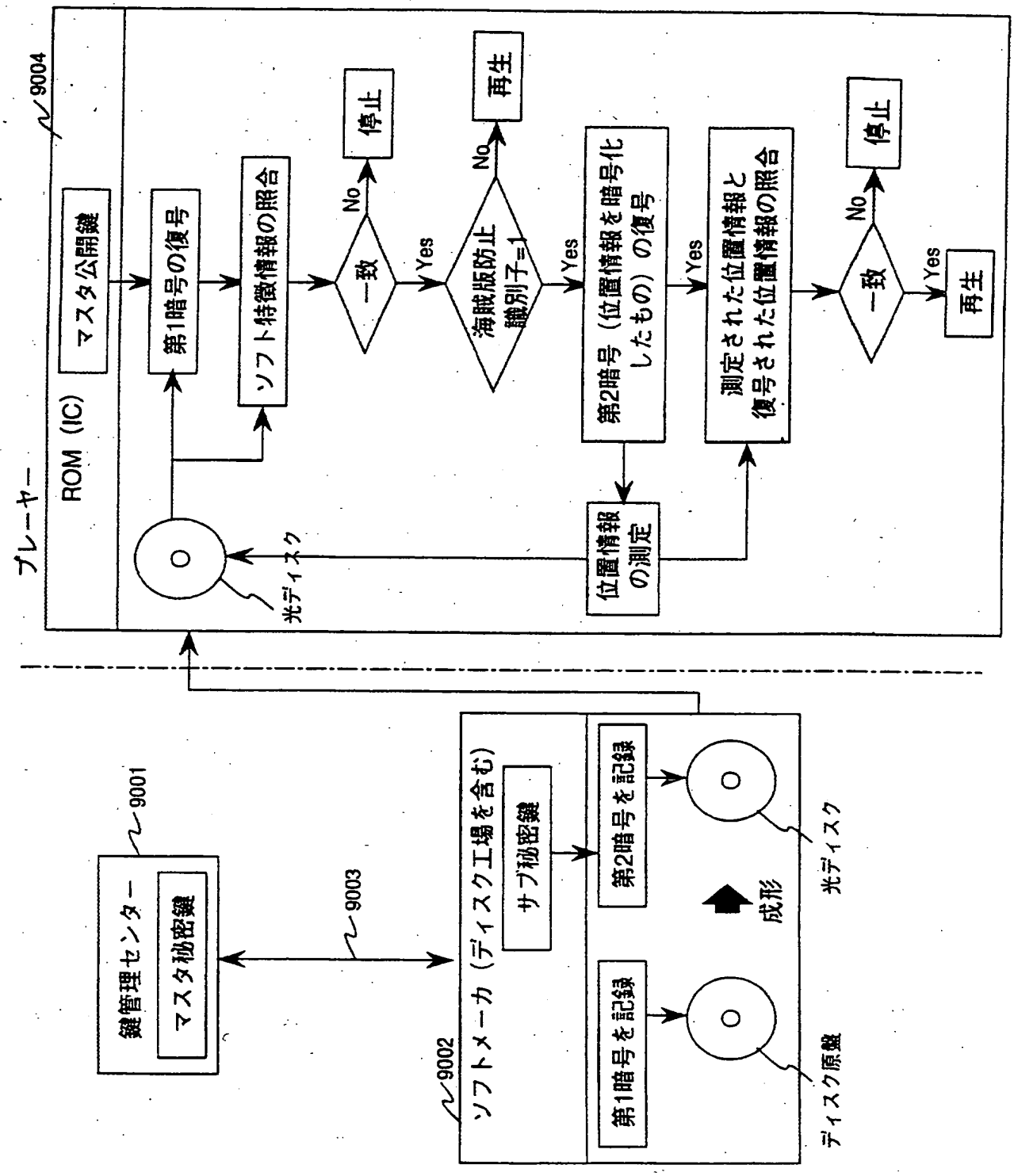
第３８図


ディスク照合ステップ
第2暗号記録部
800
876m
第2暗号の再生
876n
第2暗号の署名検証
876p
OK?
NO
STOP
Yes
マークの第1位置情報の復号
876r
マークの第１位置情報と第２位置情報の照合
876l
OK?
No
STOP
Yes
876u
RUN
876s
876g
マーキングの第2位置情報の検出
876k
サブ公開鍵 秘密鍵
ソフト照合ステップ
第1暗号記録部
800
ソフト特徴情報の照合ステップ
876a
第1暗号の再生
876b
第1暗号の署名検証
OK
NO
STOP
Yes
876h
サブ公開鍵（サブ秘密鍵）、海賊版防止識別子
第1ソフト特徴情報の復号
876c
マスタ公開鍵
876d
876e
一方向性ハッシュ関数を用いてソフトから第2ソフト特徴情報を抽出する
876f
第１ソフト特徴情報と第２ソフト特徴情報の照合
876g
OK?
No
STOP
Yes
海賊版防止フラグ=1
No
RUN
Yes

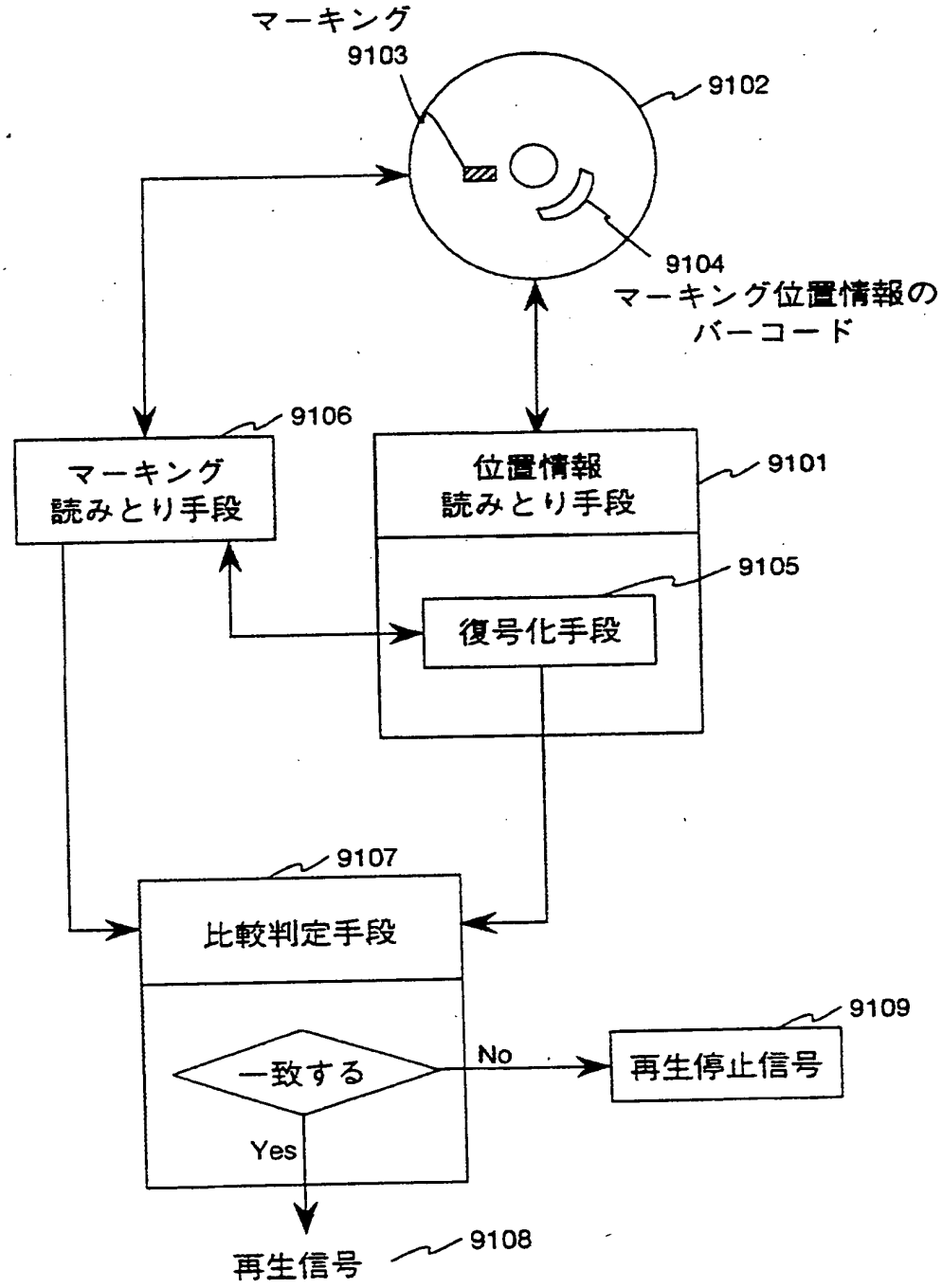
第３９図


第１世代
再生装置
881
秘密鍵系
暗号デコーダ
(8bit CPU)
878a
第２世代
再生装置
882
公開鍵系
暗号デコーダ
(32bit CPU)
878b
878c
878d
878e
正規ディスク
秘密鍵系暗号
公開鍵系暗号
879
880
照合ＯＫ
(正規再生)
RUN
NO Check
照合ＯＫ
(正規再生)
RUN
秘密鍵が破られない場合
照合不一致
STOP
秘密鍵が破られた後
照合ＯＫ(不正
再生)
RUN
NO Check
照合不一致
(不正の防止)
STOP
海賊ディスク
秘密鍵系暗号
公開鍵系暗号

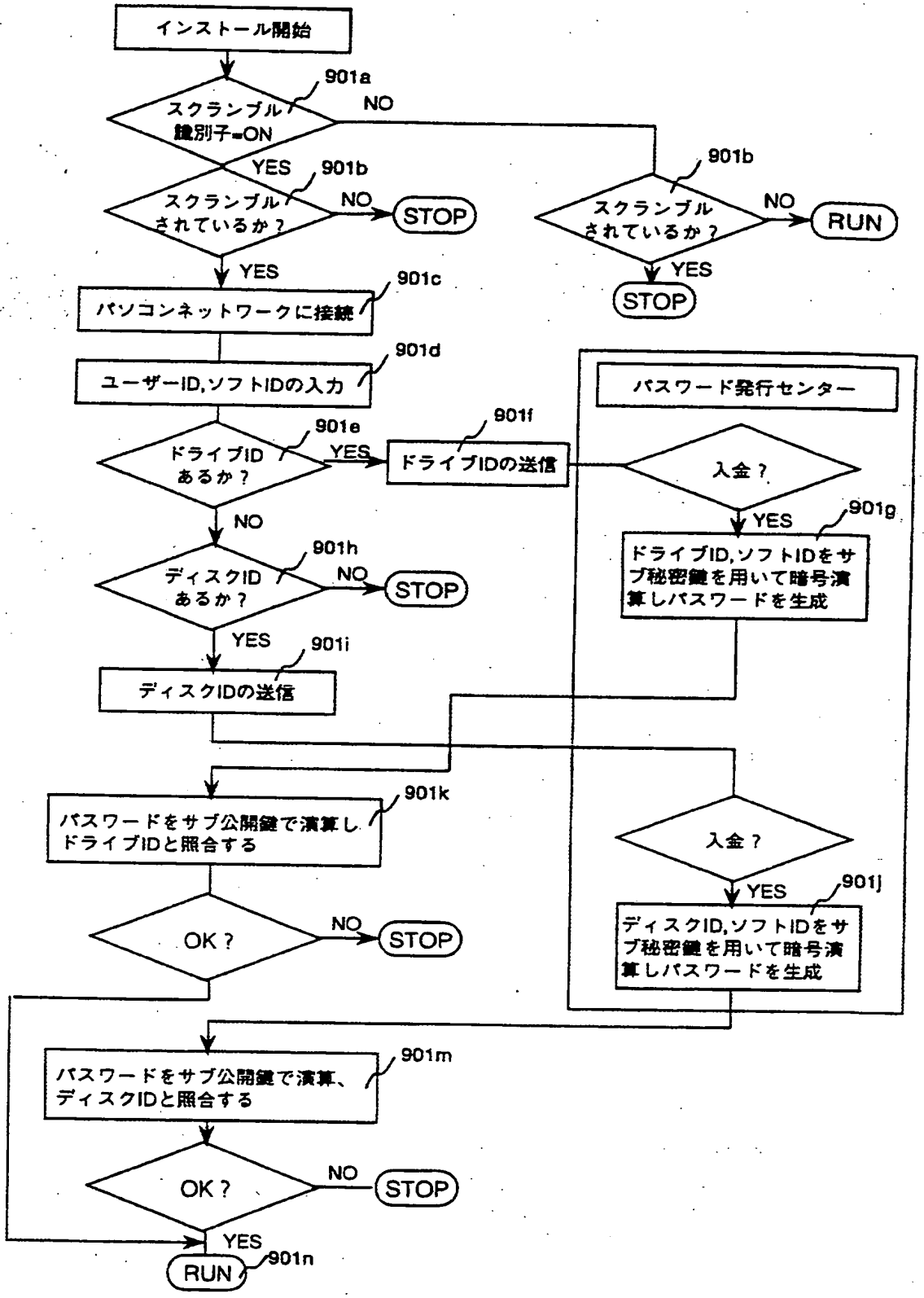
第４０図


プレーヤー
ROM (IC)
マスタ公開鍵
第1暗号の復号
ソフト特徴情報の照合
一致
No
停止
Yes
海賊版防止識別子=1
No
再生
Yes
第2暗号（位置情報を暗号化したもの）の復号
Yes
測定された位置情報と復号された位置情報の照合
一致
No
停止
Yes
再生
位置情報の測定
光ディスク
9004
鍵管理センター
マスタ秘密鍵
9001
9003
ソフトメーカ（ディスク工場を含む）
サブ秘密鍵
第1暗号を記録
第2暗号を記録
成形
光ディスク
ディスク原盤
9002

第４１図


マーキング
9103
9102
9104
マーキング位置情報の
バーコード
9106
マーキング
読みとり手段
位置情報
読みとり手段
9101
9105
復号化手段
9107
比較判定手段
9109
一致する
No
再生停止信号
Yes
再生信号
9108

第４２図


インストール開始
901a
スクランブル識別子=ON
NO
YES
901b
スクランブルされているか？
NO
STOP
YES
901c
パソコンネットワークに接続
901d
ユーザーID,ソフトIDの入力
901e
ドライブIDあるか？
YES
901f
ドライブIDの送信
NO
901h
ディスクIDあるか？
NO
STOP
YES
901i
ディスクIDの送信
901k
パスワードをサブ公開鍵で演算しドライブIDと照合する
OK？
NO
STOP
901m
パスワードをサブ公開鍵で演算、ディスクIDと照合する
OK？
NO
STOP
YES
RUN
901n
901b
スクランブルされているか？
NO
RUN
YES
STOP
パスワード発行センター
入金？
YES
901g
ドライブID,ソフトIDをサブ秘密鍵を用いて暗号演算しパスワードを生成
入金？
YES
901j
ディスクID,ソフトIDをサブ秘密鍵を用いて暗号演算しパスワードを生成

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP95/02339

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl^6 G11B7/00, G11B20/10, G11B7/26, G11B20/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int. Cl^6 G11B7/00, G11B20/10, G06F12/14, G11B7/26, G11B20/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1955 - 1995
Kokai Jitsuyo Shinan Koho 1971 - 1995

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP, 5-266576, A (Fujitsu, Ltd.), October 15, 1993 (15. 10. 93)(Family: none)	1-2, 13-14 6, 15, 25, 27
T	JP, 7-325712, A (Oki Electric Industry Co., Ltd.), December 12, 1995 (12. 12. 95)(Family: none)	3-11, 13-22, 25, 27
A	JP, 2-44448, A (NEC Corp.), February 14, 1990 (14. 02. 90)(Family: none)	1-11, 13-22, 25
A	JP, 63-46541, A (NEC Corp.), February 27, 1988 (27. 02. 88)(Family: none)	5, 8, 17, 20
A	JP, 63-164043, A (Toshiba Corp.), July 7, 1988 (07. 07. 88)(Family: none)	11-12, 23-24
A	JP, 61-190734, A (Matsushita Electric Ind. Co., Ltd.), August 25, 1986 (25. 08. 86)(Family: none)	26

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
January 8, 1996 (08. 01. 96)	January 30, 1996 (30. 01. 96)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号 PCT/JP 95/02339

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl[6] G11B7/00, G11B20/10, G11B7/26, G11B20/12

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl[6] G11B7/00, G11B20/10, G06F12/14, G11B7/26, G11B20/12

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1955－1995年
日本国公開実用新案公報 1971－1995年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y A	JP, 5－266576, A（富士通株式会社）, 15. 10月. 1993（15. 10. 93）（ファミリーなし）	1－2, 13－14 6, 15, 25, 27
T	JP, 7－325712, A（沖電気工業株式会社）, 12. 12月. 1995（12. 12. 95）（ファミリーなし）	3－11, 13－22, 25, 27
A	JP, 2－44448, A（日本電気株式会社）, 14. 2月. 1990（14. 02. 90）（ファミリーなし）	1－11, 13－22, 25

☑ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」先行文献ではあるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日
08. 01. 96

国際調査報告の発送日
30.01.96

名称及びあて先
日本国特許庁（ISA/JP）
郵便番号100
東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）
井上 信一 5D 9464

電話番号 03－3581－1101 内線 3553

様式PCT/ISA/210（第2ページ）（1992年7月）

C（続き）. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP, 63-46541, A（日本電気株式会社）, 27. 2月. 1988（27. 02. 88）（ファミリーなし）	5, 8, 17, 20
A	JP, 63-164043, A（株式会社 東芝）, 7. 7月. 1988（07. 07. 88）（ファミリーなし）	11-12, 23-24
A	JP, 61-190734, A（松下電器産業株式会社）, 25. 8月. 1986（25. 08. 86）（ファミリーなし）	26